INFORMATION AS POWER

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

VOLUME 3

Edited by
Jeffrey L. Caton, Blane R. Clark, Jeffrey L. Groh,
and Dennise M. Murphy

INFORMATION IN WARFARE GROUP, U.S. ARMY WAR COLLEGE

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
2008

2. REPORT TYPE

3. DATES COVERED
00-00-2008 to 00-00-2008

4. TITLE AND SUBTITLE
Information as Power: An Anthology of Selected United States Army War College Student Papers. Volume 3

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army War College,ATTN: Parameters,47 Ashburn Drive,Carlisle,PA,17013

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**200**	

US ARMY WAR COLLEGE

INFORMATION AS POWER

VOLUME 3

AN ANTHOLOGY OF SELECTED UNITED STATES
ARMY WAR COLLEGE STUDENT PAPERS

Faculty Review Board

Jeffrey L. Caton, Blane R. Clark, Jeffrey L. Groh,
Dennis M. Murphy, William O. Waddell, and Douglas Wake

Information as Power is a refereed anthology of United States Army War College (USAWC) student papers related to the information element of national power. It provides a medium for the articulation of ideas promulgated by independent student research in order to facilitate understanding of the information element of power and to better address related national security issues. The anthology serves as a vehicle for recognizing the analyses of Army War College Students and provides a resource for USAWC graduates, senior military officers, and interagency national security practitioners concerned with the information element of national power.

Special thanks to Harry Phillips for his significant editorial and administrative support and to Ritchie Dion for his meticulous layout editing and Jennifer Nevil for the cover design.

Information as Power

Prudens Futuri

INFORMATION AS POWER

An Anthology of Selected United States Army War College Student Papers

Volume Three

Editors:

Jeffrey L. Caton, Blane R. Clark,
Jeffrey L. Groh, Dennis M. Murphy

Information as Power

An Anthology of Selected United States Army War College Student Papers

Volume Three

Executive Agent for the Anthology:
United States Army War College

The views contained in this publication are those expressed by the authors and do not necessarily reflect the official policy or position of the United States Army War College, the Department of Defense, or any other Department or Agency within the U.S. Government. This publication is cleared for public release; distribution is unlimited.

Published January 2009.

This publication is available online at the following:
http://www.carlisle.army.mil/dime
http://www.csl.army.mil/Publications/Studies.aspx

Cover photograph by Staff Sgt. DeNoris A. Mickle, USAF. Used by permission.

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

Contents

Prudens
Futuri

PREFACE

The Information in Warfare Working Group (I2WG) of the U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2008 representing examples of well-written and in-depth analyses on the vital subject of information as power. This is the third volume of an effort that began in 2006. The I2WG charter calls for it to coordinate and recommend the design, development and integration of content and courses related to the information element of power into the curriculum to prepare students for senior leadership positions. This publication is an important component of that effort.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents, to include the 2007 *National Strategy for Strategic Communication and Public Diplomacy*, allude to different aspects of information but without a holistic, overarching strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "Use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in a complex environment consisting of the physical, information, and cognitive dimensions.

The current information environment has leveled the playing field for not only nation-states, but non-state actors, multinational corporations and even individuals to affect strategic outcomes with minimal information infrastructure and little capital expenditure. Anyone with a camera cell phone and personal digital device with Internet capability understands this. Adversary use of information as an asymmetric strategic means has been extremely effective in the current theaters of Iraq and Afghanistan leading Richard Holbrooke to famously muse: "How can a man in a cave out-communicate the world's leading communications society?"[4] And so, while it certainly is a military "superpower" one has to question whether the United States maintains that same status with regard to information.

On the other hand, the U.S. military has increasingly leveraged advances in information infrastructure and technology to gain advantages on the modern battlefield. One example from Operation Iraqi Freedom is the significant increase in situational awareness from network centric operations that enabled the military to swiftly defeat Iraqi forces in major combat operations.[5]

Clearly managing the "message" while controlling the necessary technological "means" represent critical challenges in today's information environment. We hope that this anthology will serve not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation struggles to operate effectively within this environment and to counter current and potentially future adversaries who so effectively exploit it.

Professor Dennis M. Murphy
Chair, Information in Warfare Working Group
United States Army War College

Section One

Information Effects in the Cognitive Dimension

Prudens
Futuri

Introduction

Cynthia E. Ayers
Visiting Professor of Information Superiority
Center for Strategic Leadership
U.S. Army War College

Cognitive "information effects" include words, images and actions that influence perceptions and attitudes leading to a change in behavior. Strategic communication is a way to achieve these information effects. Public diplomacy, military information operations and public affairs are considered primary capabilities (or means) of strategic communication in Department of Defense publications.

In the operational sense, informational effects are generally intended to produce specific changes in individuals, groups, and/or communities; but effects could have unexpected, unintended, and possibly undesired results. In order to minimize failure, hurdles of various kinds are placed or have been formed along the path utilized for the planning and coordination of strategic communication and messaging. Unfortunately, however, hurdles can morph into obstacles to be overcome rather than remain as useful tools for guarding against honest mistakes and ultimately, against mission failure. These induced obstacles can combine with social and cultural differences between the communicator and the intended receiver of a message, increasing the likelihood of miscommunication, misunderstanding and unintended consequences. The papers in this section concentrate on the impediments associated with strategic communication efforts, recommending changes in the manner in which the act or process of strategic communication is perceived, documented, and performed.

Colonel John R. Robinson, in his Armed Forces Communications Electronics (AFCEA) award winning paper "Mass Media Theory, Leveraging Relationships, and Reliable Strategic Communications Effects," considers the differences in effectiveness of written and verbal messages used within the context of a more "traditional" form of strategic communication and relationship-based communications. Verbalized or written forms of messaging fall short, according to Colonel Robinson, in that the effects are unreliable and reactions to messages can be unpredictable. The use of social relationships for message distribution, however, provides the dimension of conformity to societal norms, thus making effects more manageable. Although he briefly notes the need for, as well as a few of the difficulties in realistically obtaining the cooperation of "opinion-setters," Colonel Robinson argues that consistent and reliable information provided within the realm of social groupings from a presumably trusted and "persuasive leader," may provide the impetus for changes in assumptions and behavior. He uses this framework to propose a thorough review of methodologies and subsequent changes to the military's current strategic communication strategies.

Colonel Calvin C. DeWitt, in discussing legal, organizational and doctrinal impediments to the successful development of a unified strategic message in his paper: "Improving the United States' Strategic Communication Strategy," states a belief that such obstacles "are not new; they are merely more obvious in the current operational environment." He suggests that even the emotional responses inherent in the terms used to identify types of influence operations (such as "psychological operations" or PSYOP and "propaganda") can be seen as impediments to success. Additionally, he notes that inconsistencies in doctrine have confused efforts, lengthened planning time, and reduced opportunities to achieve a successful outcome. Colonel DeWitt further argues for a rethink of the specific types of organizations associated with the informational element of power as well as associated structure and manpower requirements. Ultimately, he proposes the need for legislative, organizational, and doctrinal overhaul to remove obstacles to effective strategic communication in the modern era.

Colonel Robert H. Risberg, in his paper "Improving the United States' Strategic Communication Strategy" considers a slightly broader perspective on the use of strategic communication, albeit more focused on the mission associated with the current war on terror. Colonel Risberg notes media issues, both foreign and domestic, and discusses many weaknesses similar in nature to those noted by Colonel DeWitt, but with an additional examination of "strategic listening" as referred to by Linton Wells II's House Armed Services Committee testimony of 11 July 2007. Colonel Risberg's many well-conceived recommendations include coordination of actions as proposed in Wells' testimony by a single lead agency.

Ms. Bobbie Galford considers a different aspect of strategic communication in her paper "Bridging the Cultural Communication Gap between America and its Army." Ms. Galford's stance is that "the Army is not reflective of the society it represents in relation to regional representation, affluence, education, sexual orientation and gender equality." It is becoming increasingly difficult, Ms. Galford maintains, for military members to identify with the population they are sworn to protect, and vice-versa. This lack of an exactingly representative Army (born within the context of the all-volunteer force) carries with it the potential for shortfalls in funding, political, and societal/community support, with negative media focus as one of the many unintended consequences. Ms. Galford suggests changes in recruiting tactics and enhanced strategic communication efforts with participation from both "cultures" (military and civilian) to strengthen relationships vital to national defense and address the gap she has identified.

These authors have been placed in positions where their unique experiences have influenced their perceptions and sharpened their opinions and beliefs in the ability of U.S. forces and related support organizations to achieve successful operational results. Their works hold insights and recommendations that may be crucial to the accomplishment of current and future military and diplomatic engagements.

Prudens Futuri

Mass Media Theory, Leveraging Relationships, And Reliable Strategic Communication Effects

Colonel John R. Robinson
United States Army

Words matter. It has never been clearer than in this information age that people respond to written and verbal messages in an endless mixture of ways and that the ways a sender presents information impacts the emotional response and behavior of a receiver. Because words increasingly matter, the United States military's interest in strategic communication, its potential, effects and limitations, is growing as well. There are many definitions for strategic communication, but a recent and simple explanation defines it as, "a way of persuading other people to accept ones' ideas, policies, or courses of action."[1] The usual military venues that conduct strategic communication are public affairs, information operations and public diplomacy. Today's U.S. military leaders are briefed daily on communication "messages" that are intended to effectively address whatever the most likely subjects, as assessed from mass media, that will be in the public consciousness. These written and verbal messages are critical to ensuring unity among the U.S. military's public communicators They provide a foundation for "one voice" and set conditions for a timely response to disinformation and breaking news.

This emphasis on messaging is nothing new or innovative. Since the dawn of modern mass media, national leaders have worked to capture its power and employ it to their advantage with large populations. The intense propaganda campaigns of the early 20th century show how past governments and militaries have used both truthful and sometimes twisted information in order to vilify enemies and mobilize publics in support of a national cause.[2] What has always been troubling and frustrating to public communicators, though, is that the effects from their "messages" are far from predictable. Regardless of how carefully messages are crafted and employed, people respond differently and sometimes, they do not seem to respond at all. The problem is not that messages crafted in words do not achieve effects, but rather, the effects are sometimes not what was intended, difficult to manage and difficult to assess. Partly because of this lack of reliability from messaging, one of the primary criticisms of strategic communication is that people can rarely guarantee the characteristics or timing of effects. With that in mind, areas of strategic communication that seem to have more reliability than written or verbal messaging are communication based on relationships. People tend to respond more positively to people who are of the same social and cultural groups. As examples, families respond to patriarchs and matriarchs, congregations respond to pastors, and teens respond to peers.

This paper will use known mass media and social theories to review how strategic communication that is based on relationships is more reliable than approaches that assume successful effects from messages alone. Figure 1 gives a list of referenced mass-media theories to be discussed. For the sake of clarity, "messages" or "messaging" in this paper always refers to written or verbal messages, rather than communication via action. The first three theories to be discussed all apply to message-centric communication. These theories will show how messages do in fact achieve effects, but that the effects are unreliable. The next four theories apply to relationships and will show how relationship-centric communication can achieve more reliable effects. In addition, this paper will address two final theories to show that there is no such thing as a relationship "magic bullet" that will always achieve desired effects. Although there are theories that show how relationship-centric communication is more reliable than message-centric communication, there are also theories that show how publics will only tolerate a limited amount of persuasion from mass media. Sometimes publics will use mass media to self-correct behavior in order to make society seem more "normal."

Relationships cannot replace the utility of planned messages for ensuring "one voice" among communicators or for minimizing response time to defeat misinformation. Finally, this paper will address how the information battlespace can change depending on a message-centric or relationship-centric perspective. In the end, words matter because messages in public communication are critical for unity of effort and timely response. However, relationships are also very important and a combination of messages and relationships must be considered to achieve successful strategic communication effects.

Verbal and Written Message-Centric Theories	**Premise of Theory**
Magic Bullet	Every member of an audience responds to media messages in a relatively uniform way.
Psychodynamic Persuasion Strategy	"Learn-Feel-Do" – Carefully employed information from a persuader can change the psychological structure of an individual.
Meaning Construction Persuasion Strategy	Words take on new meaning beyond the words themselves. Related to "branding."
Relationship-Centric Theories	
Media Systems Dependency	People use media because they are dependent on it in order to understand their environment.
Social Differentiation	Communication technology enables virtual subcultures to evolve according to individual interests.
Sociocultural Persuasion Strategy	"Learn-Conform-or-be-Punished" – Groups impose revised expectations on individuals, who must then conform to acceptable norms of behavior
Two-Step Flow	People are more likely to believe information from experts or authority figure persons with whom they have a trusted or perceived positive relationship.
Relationship-Centric Theories That Show Limits of Effects	
Harmony and Balance	People gravitate toward information they already believe.
Structural Functionalism	When society begins to seem chaotic, the participants of the society will take steps to reestablish social harmony.

Figure 1: List of Referenced Theories

The Search for Messaging Effects

Interestingly, the U.S. Army learned early on that message-centric public communication is not very reliable. The U.S. Army began using mass communication on an unprecedented scale during World War II and conducted significant research projects to determine media effectiveness.[3] One of these Army projects was a series of films called *Why We Fight*. The purpose of this film series was to enhance the motivation of Army recruits during training and orientation. Research on the series revealed it was very good at providing factual information, somewhat effective in changing specific opinions, but had no effect in motivating people to serve or causing them to resent the enemy. When combined with other research, the *Why We Fight* series showed that a mass communication message is unlikely to change strongly held attitudes.[4] It seems illogical then, that despite what was learned in this film series, and after years of communicating strategically, the U.S. military seems to remain heavily focused on achieving communication effects with messaging.

An indicator of how the U.S. Army came to its current approach to strategic communication occurred in the late 1990's. During this period, the missions of the U.S. military were evolving toward humanitarian and stability operations. Fire supporters at this time seemed bereft of opportunities to plan missions for lethal munitions. In the absence of lethal missions, they began planning and organizing public affairs and information operations activities as part of non-lethal fires, perhaps because fires-planning was already a well-understood management tool.[5] In other words, information for general public consumption was sometimes controlled in the same manner as non-lethal ordnance, such as smoke artillery rounds. There seemed to be assumptions at that time that using carefully prepared information alone as part of fires planning could yield timely and reliable effects. Information for public release was distilled down to the most critical themes and messages with the intent to publish them at planned times via designated media. Today, information operations and public affairs are still often categorized as non-lethal fires.

Even though it may have seemed innovative in the 1990's, the idea that written and verbal messages could be managed and employed like ordnance was not new. The "Magic Bullet" theory is an early message-centric communication theory referenced during World War I and used again in the 1930's when Paul Joseph Goebbels employed intense propaganda and messaging techniques to mobilize and maintain German public will in support of Adolf Hitler's policies. The logic behind this theory is that every member of an audience responds to media messages in a relatively uniform way, and carefully crafted information can produce immediate and direct responses.[6] Sociologists today tend to regard this theory as "naïve and simple."[7] Basically, the Magic Bullet theory only seems to be effective if an audience is already psychologically disposed to either believe the message or sincerely trust the source of the information. For example, if the theory were used by the U.S. military in Iraq, it would first have to be assumed that the population uniformly trusts information from the U.S. government. Given the complexity of Arab audiences and their varying suspicions of western motives, it is likely that any U.S. effort to employ the Magic Bullet theory in the Middle East would be a failure.

Despite the limitations of the Magic Bullet theory, researchers continue to try to find a way to tie reliable effects to messaging, because the idea of achieving valuable results with the mass distribution of words alone is just too tempting. This may be why the military today seems to employ another message-centric approach known as Psychodynamic Persuasion Strategy. The Psychodynamic Persuasion Strategy hinges on an assumption that the key to persuasion lies in effective individual learning. Many advertisers and other communicators employ this approach as though it were nothing short of common sense. The premise of Psychodynamic Persuasion Strategy is that carefully employed information from a persuader can change the psychological orientation of an individual. This theoretical reaction to information might also be described as "learn-feel-do,"[8] and is illustrated in Figure 2 (next page). Hypothetically, after exposure to carefully prepared messages, a person who has a firm suspicion of soldiers will become somewhat less suspicious and more cooperative upon learning that only a tiny percentage of American soldiers have ever committed crimes. The diagram below shows how Psychodynamic Persuasion Strategy is intended to work. Once an individual hears a persuasive message, he thinks differently, and subsequently changes his behavior.

The problem with Psychodynamic Persuasion Strategy is that researchers can not make it work reliably. Rather than learning that American soldiers are trustworthy, feeling less afraid, and then behaving in a way that is not averse to those soldiers, it is impossible to determine how the target person's suspicions of American soldiers are affected. This may be because, as researchers consistently have determined, unwanted 'boomerang' and side-effects occur because of unknown or uncontrolled variables in the target audience. These problems significantly impact the success of information campaigns, which depend to some degree on messages being interpreted in the same way as was intended by the information source. Because all individuals are different and have varying life-situations and experiences, they often react to messages differently.[10]

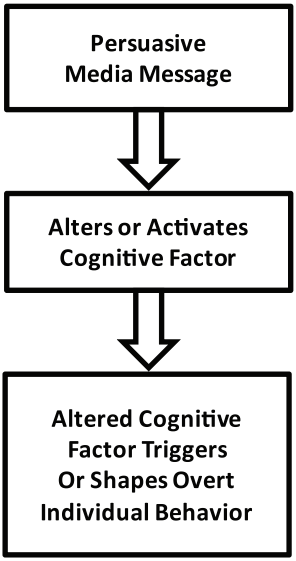

Persuasive Media Message
Alters or Activates Cognitive Factor
Altered Cognitive Factor Triggers Or Shapes Overt Individual Behavior

Figure 2: Psychodynamic Persuasion Strategy ("Learn-Feel-Do")[9]

One other theoretical approach using messaging that deserves discussion is Meaning Construction Persuasion Strategy.[11] People experience this strategy every day in the form of catchy advertising slogans and symbols that signal memory responses as to the real meaning behind words. One mobile phone company identifies itself using the term, "fewest dropped calls," while another asks, "can you hear me now?" A credit card company asks, "what's in your wallet?" and a news organization says, "we report, you decide." The Army is "Army Strong," and the Marine Corps is, "The Few. The Proud." All of these phrases are at the heart of modern branding techniques and they carry meanings beyond the words themselves. In effect, the words take on a new meaning, as seen in Figure 3.

When these slogans and brands work as intended, the meaning behind the words results in positive action, such as buying a cell phone or joining the Army. These techniques are clearly useful and effective, explaining the huge sums of money spent on advertising yearly. Once

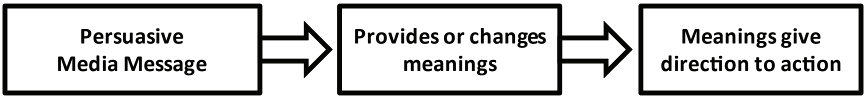

Persuasive Media Message
Provides or changes meanings
Meanings give direction to action

Figure 3: The Meaning Construction Persuasion Strategy[12]

again though, and despite the many hours that advertisers spend brainstorming for the perfect phrase that will result in widespread action or profit, the Meaning Construction Persuasion Strategy is not consistently reliable. The effects of branding may be successful for one audience or culture, but ineffective with another.

In roughly the past 100 years, there are reflections of all of these message-centric communication theories and approaches in the public communication efforts of the U.S. military. Because these message-centric techniques have unreliable effects on individuals, some information campaigns seem to be based on simple hope that broad distribution of messages will achieve intended effects on at least some members of an audience. For advocates who would manage messages as non-lethal fires, messages are the ultimate area-fire weapon. Still, the effects are unpredictable. The question is why do communicators continue to emphasize messaging in military planning? The answer already mentioned is the unity of message and the timeliness that message planning affords. In addition, it seems to be ingrained in western psyche that messages in themselves achieve consistent and reliable effects, even though they do not.[13] This may be most evident by reviewing how the U.S. military tends to view something it calls "the information battlespace."

Message-Centric Information Battlespace

Depending upon the message-centric theories to which military strategic communicators subscribe will affect how they view the information battlespace. An Internet search of "information battlespace" yields many different ideas about the environment of public communication and how that environment is affected. Generally, though, the view of the information battlespace that many in the U.S. military employ is an ever-changing domain of data that is continuously impacted by a large variety of influencers.[14] These influencers include the White House and other global executive bodies, Congress, other agencies and foreign governments, various militaries and related institutions such as the Northern Atlantic Treaty Organization, the United Nations, infinite media organizations, bloggers, and so on. The way to persuade people in this constantly changing information domain is to dominate the news cycle with high-interest events, appealing visuals, and well-crafted messages in order to achieve a cognitive effect with audiences. The characteristics of an information battlespace that is nebulous and ever-changing include effects that last only as long as a subject remains in the mind, or cognitive domain, of the media and public. This means there is often constant anxiety among public communicators over which influencing agent has managed to dominate the news cycle. A videotape of Osama bin Laden that is released by al Qaeda to the general public may be considered a significant win for the enemy and the organization that first publishes that videotape, perhaps al Jazeera, is suspected as an al Qaeda sympathizer. Mass media analysts and researchers conduct endless assessments on the number of times specific "messages" are published in the press and these numbers are sometimes presented as metrics for success or non-success.

Because the mass-media theories that have been discussed thus far show that messages do not guarantee reliable effects, it is troubling that the U.S. military's strategic communication community views its information battlespace as just the opposite, a place that is constantly fluid and changing, but where effects can be reliably achieved. It is no wonder there is so much frustration. The U.S. military's constantly changing information battlespace, where messages are not reliable, might be akin to fighting the biggest tar baby ever imagined, or worse, trying to shape a world made of goo.

Theories that Point to Relationships

One place to start when researching for mass media theories that are more sophisticated than the Magic Bullet theory, and more reliable than other message-centric approaches, is to determine how and why people use media in the first place. The Media Systems Dependency theory asserts that people use media because they are dependent on it in order to understand their environment. In a sense, people establish relationships with their preferred media. Watching news and entertainment on television, listening to the radio, reading newspapers and books, and of course surfing the Internet, all contribute to an individual's complete understanding of the world.[15] At the same time, media are dependent on audiences because it is each individual who chooses which media are useful and reliable. However, if a person ever comes to believe that a media source is no longer a trustworthy source of information, he or she will choose a different media system that they perceive as more credible. The implications of the Media Systems Dependency theory for the military are very serious, because it indicates how public information must have long term credibility in order to be strategically effective. Any information accredited to the U.S. military that is somehow proven to be fallacious or biased can ruin the military's relationship with an audience for as long as it takes to reestablish trust. Given the pervasiveness of public communication in today's world, the fallout from false information grows exponentially as information is passed from media to media.[16] Public information that intentionally deceives enemies can also deceive allies, all of whom have the potential to choose other sources of information once the deception is revealed. As one source explains it, "Everything in the realm of strategic communication should be as truthful as human endeavor can make it. Tell the truth even though sometimes, for security, you can't tell the whole truth."[17]

Because people seem to establish forms of relationships with media, the Media Systems Dependency theory's approach to why people choose media has a very important connection to another useful theory know as Social Differentiation. The Social Differentiation theory contends that people increasingly choose communities of interest, rather than geographical communities. The result of willingly organizing into communities of interest is people separating into virtual subcultures based on whether they are liberal, conservative, athletic, academic, homosexual, Christian, Islamic, and so on.[18] The obvious modern-day medium between social differentiation and media is the internet, which has enabled virtual subcultures to evolve dynamically according to individual interests. For instance, a man with a strong interest in hunting will seek out other people who like hunting. He might establish new relationships with other hunters using Internet chat rooms and newsgroups and these friends will tell him where to find the finest hunting equipment, as well as the best places to hunt. Because of shared interests and lifestyles, this hunter could eventually have more developed relationships with his online hunting friends than with his own next door neighbors. Therefore, when public communicators seek to be more influential by establishing relationships with audiences, it is important to consider the norms, interests and media of various subcultures, and adjust engagement techniques accordingly.

To some degree, by taking steps to communicate with differing audiences according to what media is preferred, the U.S. military is already operating in the realm of social differentiation. Blogging, podcasting, web communication, television, radio, and installation newspapers are all used by the U.S. military to reach different subcultures. Still, if the military fails to remain a credible source of information using any particular medium it has invested in, the Media Systems Dependency theory indicates that the subcultures tied to that medium are potentially lost to the military for an undetermined period of time in lieu of other, more credible sources of information. When applied to the Middle East, the implications for the U.S. military are very severe. If subcultures perceive media that present the U.S. military's information as less credible than an adversary's media, the U.S. military potentially loses those subcultured audiences to media that report an enemy's points of view.

Critical to the ideas behind Social Differentiation theory, and the possible persuasive powers of subcultures, is the importance and influence of individual sociocultural relationships. It was mentioned at the beginning of this paper how the military sometimes seems to use the approach of Psychodynamic Persuasion Strategy in its public communications resulting in a "learn-feel-do" explanation for how people are persuaded. Even though this approach seems like common sense, researchers have an abundance of evidence to suggest that individuals are actually more persuaded by social expectations than by direct messages. Most people have heard of "peer pressure" for instance, and its influence on the behavior of teens. So, as an example, in a community where soldiers represent a key means of security or income, a person who dislikes and criticizes soldiers in that social environment might, in turn, be humiliated or belittled by other members of the local society. In this example, the individual stops criticizing soldiers because the group imposes a sort of "learn-conform-or-be-punished" approach, called the Sociocultural Persuasion Strategy, rather than a "learn-feel-do"approach.[19] As seen in the diagram below, when a group responds to information, perhaps from a persuasive leader, the values and norms for the group can change. In turn, the group imposes revised expectations on individuals, who must then conform to acceptable norms of behavior.

The key difference between this strategy and Psychodynamic Persuasion Strategy is that researchers have more than enough evidence to show that it works. Generally, the social groups that people interact in, whether family, schools, churches, clubs or cliques, have enormous influence over what is and is not normal, acceptable and expected behavior.[21]

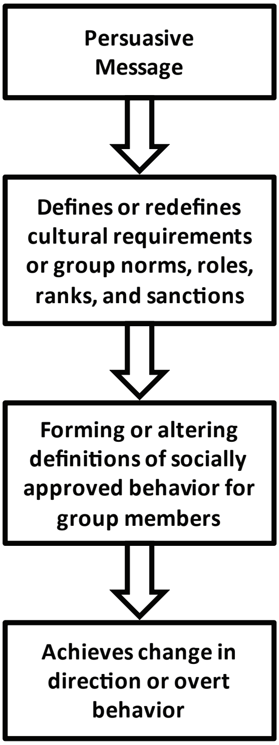

Persuasive Message
Defines or redefines cultural requirements or group norms, roles, ranks, and sanctions
Forming or altering definitions of socially approved behavior for group members
Achieves change in direction or overt behavior

Figure 4: Sociocultural Persuasion Strategy ("Learn-Conform-or-Be-Punished")[20]

Society has endless examples of how group pressure is leveraged to change behavior, from the use of Alcoholics Anonymous as an effective means of combating drinking, and "Smoke Out" day to discourage cigarette use, to heavy publicizing of the "Run for the Cure" to encourage activism on behalf of breast cancer cures.[22] Simply, the power of social and cultural groups within public communication is extraordinarily significant. When applied to how the U.S. military communicates and changes opinions among populations, community relations and civil affairs techniques become very important tools within the Sociocultural Persuasion Strategy framework. Events and actions that emphasize well-being and respect for groups have the potential to, sequentially, influence the behavior of single individuals.

Because group pressure is so persuasive on the behavior of individuals, the challenge for the U.S. military is determining how to establish, reestablish or improve linkages with key audiences or subcultures. The concept of Two-Step Flow is a theory that at least provides a starting point to persuading groups. The Two-Step Flow theory asserts that people are more likely to believe information from experts or authority figure persons with whom they have a trusted or perceived positive relationship, such as a pastor, parent, trusted journalist, or like-minded politician.[23] This theory is about engaging and networking with opinion-setters who have the capacity to impact the attitudes of secondary audiences. As an example, the late Jerry Falwell often used media to inform his Evangelical Christian followers. When something appeared in the news that was controversial to Falwell's followers, they might reserve their opinions until hearing what Falwell had to say about the subject.[24] When the Two-Step Flow is tied to Social Differentiation, it is clear that identifying the opinion-leaders for a variety of subcultures is key to impacting the behavior of larger and more general audiences. The Ayatollah Sistani, for instance, is a critical opinion-setter that the U.S. military must consider to gain a positive relationship with many Shi'ites in Iraq. Likewise, Muktadr al-Sadr is another opinion-setter for the Shiite Mehdi Militia subculture in Iraq and the U.S. military has already shown that it must decide whether to silence or persuade al-Sadr in order to change the behavior of the Mehdi Militia.

Relationship-Centric Information Battlespace

The four relationship-centric theories discussed in the section above show that strategic communication effects derived from relationships tend to be more reliable than message-centric effects. It is important to discuss how a relationship-centric information battlespace differs from the message-centric information battlespace that was discussed earlier. The information battlespace for a communication strategy that is focused specifically on relationships is less fluid. It is not a domain of ever-changing data. Rather, the battlespace for relationships is, simply, people. As seen in the Sociocultural Persuasion Strategy, people consistently respond to the pressures from their associated groups and often conform to the behaviors of a group even if they do not personally believe in that behavior. In a battlespace of people, there is less concern over dominating the information domain and a more targeted focus on information that can affect the core opinions of groups and subcultures. An individual who hears a particular message may never change behavior in the way intended by the sender, even if he hears the message repeatedly. However, if a group as a whole is persuaded, perhaps through the influence of group opinion-leaders, then the individual may be persuaded as well. Researchers have determined that, "many longer-term effects of mass media do not involve the intentional or immediate audience at all, but are the secondary responses of others."[25] Finally, analysis of an information battlespace of people is less about the number of times a message appears in the media and more about an assessment of cultural norms, behaviors and opinions on issues in response to detailed study, surveys, focus groups and other similar types of research.

Relationship-Centric Theories That Show Limits of Effects

Despite having more reliable effects, relationship-centric theories do not offer any "Magic Bullet" of their own. There are also theories that highlight realistic limitations to the potential effects of relationship-centric communication. First, related to the Two-Step Flow is the Harmony and Balance theory, which asserts that people gravitate toward information they already believe. In other words, audiences do not want to be challenged by new information or controversial ways of thinking. Audiences instead seek out other people with whom they already agree.[26] Most Rush Limbaugh listeners, for instance, listen to him because they have already decided in favor of the things that he says, not necessarily because Rush Limbaugh is autonomously empowered to significantly change the opinions of large audiences. The implication behind Harmony and Balance theory for the U.S. military is that it cannot be assumed that subculture members who have controversial leaders are simple-minded or easily swayed. Rather, it is more likely that subculture members have identified with a group and leader that already reflect their acceptable norms and beliefs. Referring back to al-Sadr and the Mehdi Militia in Iraq, some people might say that al-Sadr can mobilize the Mehdi Militia because he speaks forcefully for a community that has suffered oppression in Iraq. However, Harmony and Balance explains that many Shiites in and around Baghdad are sympathetic to al-Sadr's political and religious opinions because they already share similar views.

A second theory that reveals the limits of effects from relationship-centric communication is Structural Functionalism. The concept behind the Structural Functionalism theory is that the organization of society is the source of its stability and each category of society's participants contributes to the attainment of social harmony.[27] When society begins to seem chaotic, the participants of the society will take steps to reestablish social harmony. When applied to mass media, Structural Functionalism indicates that audiences that are experiencing chaos will prefer media that reflect a return to social harmony. American television programming from the 1960's and 1970's are possible examples. Television audiences might have preferred "The Brady Bunch," "The Waltons," and "Happy Days" because these shows reflected ideal families with normal behavior. Applied to the chaos of current Iraqi society, Structural Functionalism would assert that many Iraqis will prefer media that point to a return to an Iraqi view of social harmony. In other words, some Iraqis might prefer media that identify with traditional values and strict interpretations of Islam, reflecting a desire to return to historically stable governments in Islamic history. Structural Functionalism's challenge for the U.S. military is how to best present Iraqis with a path to social harmony that does not require a return to non-democratic, oppressive forms of Islamic government.

Discussion and Recommendations

The first thing that should result from reading this study is realization that messages alone are not sufficient for planning and achieving reliable strategic communication effects. Messages are critical to unity of intent among various communicators, achieving "one voice" and responding quickly in order to address breaking news and disinformation. But messaging effects are not reliably consistent or controllable. On the other hand, effects from relationship-centric communication are much more reliable. Unfortunately, at the same time that U.S. military strategic communicators seem heavily focused on gaining effects via messaging, there seems to be few mechanisms for harnessing relationships. Those that exist appear primarily in the civil affairs and public affairs (community relations) arenas, as well as various engagements with military support to public diplomacy.[28] The community relations parts of public affairs are currently very focused on enhancing the U.S. military's image in U.S. local communities through bands, capability demonstrations, speakers bureaus, and similar venues, but do not necessarily operate along synchronized paths to achieve strategic effects. In order to become more effective, the U.S. military's strategic communication efforts should evolve in planning and execution to include effects via relationships, both personal and public. These identified relationships should include government, community, media and opinion leaders that have the capacity to impact audiences on a local, national and international level. Planning should also address the sociocultural norms that drive these audiences, as well as reasonable goals for impacting audience behaviors. Because public affairs is the only strategic communication capability that communicates directly to U.S. citizens, the community relations capabilities of U.S. military public affairs should be expanded and refined.

The second point the reader should glean from this study is that the U.S. military's information battlespace is much more manageable and understandable if viewed from a relationship-centric rather than message-centric perspective. An information battlespace that is centered on relationships is less fluid and enables communication techniques that have more reliable effects. The attitudes and beliefs of people evolve over time. Therefore, a people-oriented information battlespace does not immediately change or justify panic just because a strategic communicator makes a mistake or an enemy proves able to publish his message. On the other hand, a message-centric battlespace is hardly manageable, precisely because it is ever-changing with new information and because the effects from messages intended to change the battlespace are themselves unreliable. As a result, the U.S. military should reexamine if its current view of the information battlespace is useful and appropriate. Choosing to view the information battlespace from a relationship-centric point of view would require communicators to think about strategic communication in entirely new ways. One, because relationships require time to evolve, the effects and expectations from strategic communication would be less immediate. Two, strategic communicators would have to operate according to information that goes well beyond what is being "said," so that decisions are also based on what is being "done." Third, analysts in a relationship-centric battlespace would have to focus less on how many times certain information appears in the mass media and more on identifying key personalities and influencers, as well as, their agendas, preferences, characteristics and personal interests.

The third point from this paper stimulates the question whether or not the U.S. military is adequately prepared to conduct successful strategic communication that is based on relationships. A military that is predominately focused on achieving victory through combat may not be correctly postured to achieve victory in the information battlespace. This means that the U.S. military must critically review its programs for language and cultural training, as well as for strategic communication training, to ensure that leaders can succeed in a non-lethal, relationship-centric information battlespace. Finally, the U.S. military must seriously review its own relationship with the U.S. State Department, determine precisely what all the military's role is in diplomacy, and enable better linkages between foreign affairs officers and other strategic communicators.

Conclusion

In summary, even though the U.S. Army learned during World War II that message-centric public communication is not a reliable means of gaining desired effects, most of its communication efforts still seem to work from a message-centric point of view. The Magic Bullet theory, Psychodynamic Persuasion Strategy, and Meaning Construction Persuasion Strategy all demonstrate that written and verbal messages have effects, but that these effects are not reliable. On the other hand, communication that harnesses relationship linkages is much more reliable. The Sociocultural Persuasion Strategy shows that groups have the power to influence individual behavior, as seen in families, churches, schools, businesses and communities. The Two-Step Flow explains that the leaders of these sociocultural groups have the ability to influence the behavior of associated communities and subcultures. Once these and the other discussed theories are fully understood, the challenge for the U.S. military is determining how to establish, reestablish or improve strategic communication with key audiences or subcultures and their leaders. Ultimately, strategic communicators have to develop both synchronized messaging and savvy management of relationships to achieve unified and reliable strategic communication. In his classic guide, *How to Win Friends and Influence People*, Dale Carnegie suggests that the only way to get anybody to do anything without forcing them is by making them want to do it.[29] The way to make them want to do something is by determining and offering what they need or desire. Similarly, the late Speaker of the House of Representatives, Thomas P. "Tip" O'Neil, is oft remembered for saying, "All politics is local." His own success indicates he knew that one must demonstrate true concern for the well-being of voters in order to gain their support. These classic communicators understood that extraordinary powers of persuasion very often result from having a real or perceived positive relationship with individuals or larger audiences. Perhaps it is time for the United States military to do the same.

Strategic Communication, Psychological Operations and Propaganda: Is a Unified Strategic Message Possible?

Colonel Calvin C. DeWitt
United States Army

Retired Marine Colonel Thomas X. Hammes suggests that modern warfare has evolved significantly beginning with Mao's tenants and progressing to the first Intifada's success in using mass media to challenge Israel's military power. He argues that warfare has "shifted from an Industrial-Age focus on the destruction of the enemy's armed forces to an Information-Age focus on changing the minds of the enemy's political decision makers."[1] Yet in spite of this evolution, United States Strategic Communication is among the most misunderstood and misapplied principles in government today. Strategic leaders and planners recognize a coordinated national message is a necessary condition for achieving U.S. Government (USG) objectives, but efforts to develop centralized programs and plans continue to fall short, and attempts to orchestrate messages across the broad interagency spectrum have been uniformly unsuccessful.

It is fashionable to point out that 9/11 did not change the threats faced by the United States and its allies, it simply forced these governments to focus on the real challenges at hand. By the same token, the impediments to the development of a unified strategic message are not new; they are merely more obvious in the current operational environment. The existing impediments to success are threefold. The first is legal, or the way in which laws and statutes are currently understood. The second impediment is organizational, that is, the government and its supporting departments and agencies are organized in such a way that coordinated Strategic Communication is all but impossible. And finally, there are numerous doctrinal impediments to coordinating themes and messages within the Department of Defense (DoD).

If coordinated and synchronized, strategic themes and messages become elemental to winning a fourth generation war. Impediments to effective Strategic Communication must be identified, analyzed, and changed before the USG can effectively engage foreign populations and shape behavior in a manner that furthers U.S. national objectives.

A Problem of Definitions

Psychological Operations (PSYOP) and propaganda are two words that remain problematic in any discussion surrounding United States' attempts to engage foreign publics. The DoD defines propaganda as "any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly." PSYOP are those "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals." Adding that "the purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives." By these definitions, PSYOP are the act of planning, preparing, and distributing propaganda to foreign audiences. But propaganda is a word commonly associated with lies, thereby creating a problem because the USG does not want to admit to its citizens – or itself – that it conducts propaganda. As a result, professionals in and around the military prefer to use the less specific term "information operations" (IO), under which PSYOP is included as one of several capabilities. Colonel Curt Boyd points out, "So thoroughly inculcated is this misuse of [the terms IO and PSYOP] that it is now common to hear the military's most prominent leaders, including most flag officers, senior Pentagon officials, and others, routinely and improperly use IO and PSYOP interchangeably."[2] All this is to say that there exists a great deal of sensitivity and confusion around the terms used to discuss U.S. efforts to influence favorably the people and leadership of other nations.[3]

Recognizing that it is impossible, without offending the sensibilities of some segment of the public, to discuss the challenges of effectively and constructively engaging the people of other cultures, this paper will use the words propaganda and PSYOP in a generic sense to describe any factual communication produced by a government to promote national interests.

It is also necessary to define the term Strategic Communication, which means different things in different organizations, often being used a synonym for IO, PSYOP, or public diplomacy. *The Quadrennial Defense Review (QDR) Strategic Communication Execution Roadmap,* published in late 2006, calls Strategic Communication "focused USG *processes* and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs and *actions* synchronized with other elements of national power" [author's emphasis]. The inclusion of the word "processes" suggests that Strategic Communication must be planned, while including "actions" recognizes that the message must be coordinated with events on the ground. This is the broadest of definitions of Strategic Communication, but necessarily so. Only by planning the synchronization of words and deeds can the United States truly be communicating strategically.[4]

Legalistic Impediments to Strategic Communication

The United States has historically used propaganda to influence domestic and foreign publics during wars and international conflicts. In fact, the need to propagandize stems from three very American characteristics. First, Americans feel a need to explain their positions to the rest of the world, especially with regard to why their nation is engaged in war. There is a national need for moral justification of our foreign policy. Second, Americans believe in the power of advertising and are good at it. And third, there is a reluctant acceptance that psychological warfare is a justifiable weapon in war, certainly preferable to the use of lethal force.[5] The use of propaganda to justify activities, however, directly conflicts with an innate distrust among Americans of a strong central government, which is presumed to tend toward the control of its citizenry. For this reason any suggestion that the USG is intentionally propagandizing Americans provokes a strong and immediate response. Historically, this tendency is played out in the legal and legislative battles surrounding United States' attempts to coordinate a clear national message.

During World War I, George Creel headed an organization dedicated to influence domestic and foreign attitudes. Creel's Committee on Public Information encouraged hatred of Germans and encouraged the American public to report suspicious behaviors. The committee came under criticism for its intent and the tactics it employed, but similar programs were initiated during World War II. And while United States' propagandizing and censorship were again criticized, it was the German government's anti-Jewish and pro-Nazi propaganda that drove the strongest sentiment against propaganda in the United States.

Congress understood American distrust of government, especially a strong executive, and charged the State Department with overseeing international public relations. To that end, they passed the United States Information and Educational Exchange Act, or Smith-Mundt Act, to "promote a better understanding of the United States in other countries, and to increase mutual understanding between the people of the United States and the people of other countries."[6]

To promote this mutual understanding the State Department created student and professor exchanges between the United States and other nations. But the act also authorized the "dissemination abroad" of information about the United States through electronic and print media, as well as through information centers. The effort was clearly driven by the realities of the Cold War and a corresponding desire to engage the Soviet Union in a war of words and ideas. While the effort can be characterized as propagandizing, Secretary of State George C. Marshall, among others, understood that the information would have to be truthful to maintain any degree of credibility.[7]

It is important to note the original act did not contain an explicit ban on propagandizing Americans. It actually made such information available in English "following its release as information abroad [to] press associations, newspapers, magazines, radio systems, and stations…"[8] Indeed, such public access to the products of U.S. international expression would arguably be a uniquely American right. However, belief in a right to see this propaganda was balanced with the concern that the difference between providing access to the products and overtly propagandizing the U.S. public was too fine a distinction. As a result, the Smith Mundt Act and its subsequent amendments had the effect of preventing public distribution of propaganda products.

The U.S. Congress has traditionally sought to limit the extent of the government's direct influence on its citizens, and as such has interpreted the Smith Mundt Act as a law supporting this view. By contrast the executive branch supports a more literal interpretation of the law, seeing few specified limitations and arguing that the government has a right – and perhaps responsibility – to inspire their citizenry in support of national objective. This tendency has been repeatedly demonstrated, including efforts by the Clinton administration in the form of the International Public Information System, which sought to counter anti-U.S. propaganda, and again by the second Bush administration's short lived attempt to form the Office of Strategic Influence in the DoD.

Allen Palmer and Edward Carter, two lawyers writing in *Communication Law and Policy*, point out that most challenges to the ban on dissemination of propaganda in the U.S. on the grounds of either the First Amendment or the Freedom of Information Act have been unsuccessful, resulting in the ban being upheld. They argue against the ban, however, primarily because technology has made the ban unenforceable.[9] In an interconnected world, propaganda aimed at the foreign population is easily accessed on the Internet, even if that was not its original format. More importantly the ban conflicts with longstanding U.S. tradition of advocating the free flow of information across borders. A similar principle holds that citizens should in most cases be allowed to know what their government is doing in their name.

In spite of the original reason for the Smith Mundt Act, i.e. telling America's stories abroad, legal precedent seems to favor upholding a ban on domestic dissemination of propaganda. As a practical matter the law has become unenforceable, but there is ample reason for revisiting the legislation to ensure it supports U.S. objectives at home and abroad. The law could be adjusted to preclude government influence activities from intentionally targeting the U.S. public while making it clear that regular communication with foreign audiences must be factually true and consistent with U.S. values. But this restriction must be balanced against the traditional principle of open communication across boarders and the presumption that U.S. citizens should generally have access to such unclassified, albeit sensitive, communications. As such, propaganda should be made available to the U.S. public.

Organizational Impediments to Coordinating Strategic Communication

The second impediment to a unified strategic message is organizational. The dissolution of the United States Information Agency (USIA), which for decades served to ensure the USG spoke with one voice, has contributed to an inability to present a single message across government agencies. Attempts to rectify the situation, including the short-lived Office of Strategic Influence and the position of Under Secretary for Public Diplomacy and Public Affairs (USPDPA), held until December 2007 by President Bush's close advisor Karen Hughes, have both fallen short. This failure has prevented the effective coordination within the USG of the information instrument of power.

The USPDPA had three long term strategic objectives under Ms. Hughes:

- Offer people throughout the world a positive vision of hope and opportunity that is rooted in America's belief in freedom, justice, opportunity and respect for all.

- Isolate and marginalize the violent extremists; confront their ideology of tyranny and hate. Undermine their efforts to portray the west as in conflict with Islam by empowering mainstream voices and demonstrating respect for Muslim cultures and contributions.

- Foster a sense of common interests and common values between Americans and people of different countries, cultures and faiths throughout the world.[10]

Hughes's goal was to become more effective in six areas including: exchange programs, recognizing and responding to global news and informational trends, defining and conducting public diplomacy, private sector partnerships to make America more accessible to foreign audiences, communications technology, and de-legitimizing terror.[11] And while Ms. Hughes's intent was noble, there is little indication these efforts produced a positive impact. To the contrary, some analysts believe she was largely ineffective. More than any time since the USPDPA was formed, foreign audiences are questioning the assumption that America has respect for other cultures, mainstream Muslim voices are being marginalized by Sunni and Shia extremists, and differences between cultures and religions are being accentuated. There is clearly a perceived distinction in the Muslim world with respect to America's message and her actions. And while it is true that making an impact with limited resources against the backdrop of the entirety of American popular culture is a difficult task, Ms. Hughes's decision to take on the role of public diplomat herself, rather than build, train, and empower an organization to achieve the desired effects was roundly criticized.[12]

Similar criticism has come from within the government as well. The Government Accountability Office (GAO) reported on three occasions that the USG does not effectively integrate its diverse public diplomacy activities and lacks an interagency communication framework that guides these activities. The Department of State (DoS) is credited with focusing efforts on marginalizing extremists and promoting shared values, but they are criticized by the GAO for not issuing clear guidance on how to implement these objectives and for lacking elements of a communication strategy that would be found in the private sector.[13]

Analysts inside and outside government agree that a strategic direction is needed. A DoS report notes that transformation will require a "new clarity and strategic direction for public diplomacy."[14] Yet throughout the document this new strategy remains noticeably absent. In fact, the strategy alluded to seems to be to better explain American values and national interests, which is certainly nothing new. Similarly, the tactics do not seem to be new or particularly inspired: engage foreign audiences, be present, and tell America's side of the story. The report does repeatedly point out that currently modest funding levels are "absurd and dangerous."[15] One valuable addition to the public diplomacy discussion is a call for a "culture of measurement" within the State Department.[16]

Stephen Johnson and Helle Dale maintain that the USG has lost its voice since a 1999 reorganization of government agencies placed the independent USIA within the State Department. They argue that the Bush administration, while recognizing a problem with the nation's global image, has failed in their efforts to formulate and coordinate messages to foreign audience. Johnson and Helle join others in citing the DoD's inability to merge public affairs and information warfare capabilities as a contributing factor in the failure.[17]

Another recent recommendation for improving American attempts to communicate with foreign audiences included enlarging the current USPDPA structure by placing two offices directly under the Under Secretary. The Office of Resources and Management would include International Information Programs, Cultural Affairs, and the Public Affairs Bureau, while the Office of Policy and Strategic Communication would coordinate with the White House and between departments. Such an expanded capability would enable the requisite coordination, and perhaps more importantly, provide a central point for policy and budgetary requirements.[18]

Henry Hyde, chairman of the House International Relations Committee attempted unsuccessfully to revive and expand the USIA. Creating and training a force of independent diplomats capable of coordinating and synchronizing U.S. Strategic Communication efforts is a good start, but this effort must reflect a commitment to synchronized communication in the White House and in every department, especially the DoD, which is often the first, largest, and most devastatingly uncoordinated messenger on foreign soil.

The lack of coordination between departments and agencies is exacerbated by the organization of Strategic Communication efforts within the DoD, an organization, which by virtue of its size and reach is responsible for communicating with foreign audiences that would most benefit from a better understanding of U.S. policies. Inside the Pentagon, the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) is tasked with monitoring the

DoD Information Operations programs[19] while the Assistant to the Secretary of Defense Special Operations/Low Intensity Conflict & Interdependent Capabilities (ASD SO/LIC & IC) website sites U.S. Special Operations Command's (USSOCOM) *2007 Posture Statement* in claiming both Information Operations and PSYOP as activities his office is charged with supervising.[20] This division of responsibility is mirrored at the Combatant Command level, where U.S. Strategic Command (USSTRATCOM) "is a global integrator charged with the...Information Operations [mission]"[21] while USSOCOM has the authority for conducting trans-regional PSYOP.[22]

Some within DoD have recognized the problems created by this dispersion of responsibility. The department has taken the first steps toward coordinating Strategic Communication by making it a shared responsibility of the Deputy Assistant Secretary of Defense (Joint Communications), who falls within the office of the Assistant Secretary of Defense (Public Affairs), and the Deputy Assistant Secretary of Defense (Support to Public Diplomacy), who falls under the office of the Under Secretary of Defense (Policy).[23] Such coordination will be useful in synchronizing the words and deeds within DoD, but success will depend upon how these efforts are nested with national guidance and the degree and scope of interaction between both Deputy Assistant Secretaries.

Attempts to improve Strategic Communication at DoD notwithstanding, the U.S. Army public affairs community has contributed to increased confusion within the Army. The Chief of Public Affairs, who falls under the Chief of Staff of the Army (CSA) and outside of both USSTRATCOM and USSOCOM, claims responsibility for Strategic Communication within the Army. The Army 2008 Strategic Communication Guide, however, has little to do with Strategic Communication as defined above with focus on foreign audiences. Army Strategic Communication is a public affairs product designed to elicit support for the Army's mission from Soldiers, the American people, and Congress, and communicate relevant information to Soldiers. This guidance focuses on the Army's Title X responsibilities of recruiting, growing, and training the army, and on modernizing equipment.[24] It clearly does not address the interests, policies, and objectives of the USG as suggested by the DoD Dictionary of Terms. The 2006 Quadrennial Defense Review Report (QDR) does not define Strategic Communication (a spin-off "roadmap report does this), but the report acknowledges its importance in building trust and credibility with friends and adversaries.[25] If a coordinated Strategic Communication effort is a necessary condition for this trust and credibility, it is not coordinated effectively within the DoD.

At the operational and tactical level, the DoD organization further hampers effective Strategic Communication. Given the nature of what the CSA describes as an "era of persistent conflict" in which the military is currently engaged, the alignment of active component PSYOP forces within SOCOM presents an ongoing challenge within DoD. In 2006 Army PSYOP forces were split along component lines, with the reserve component PSYOP forces leaving USSOCOM and falling under U.S. Army Reserve Command (USARC). The rationale for this alignment is that these active component PSYOP forces must focus their support on deployed Special Operations units. In fact, much of the support the active duty 4th PSYOP Group (POG) provides is print and electronic media products for the interagency community. Only one battalion of the nine in 4th POG has a traditionally tactical mission. The bulk of PSYOP support to conventional forces comes from reserve units with little or no ongoing relationship to the unit they support in combat.

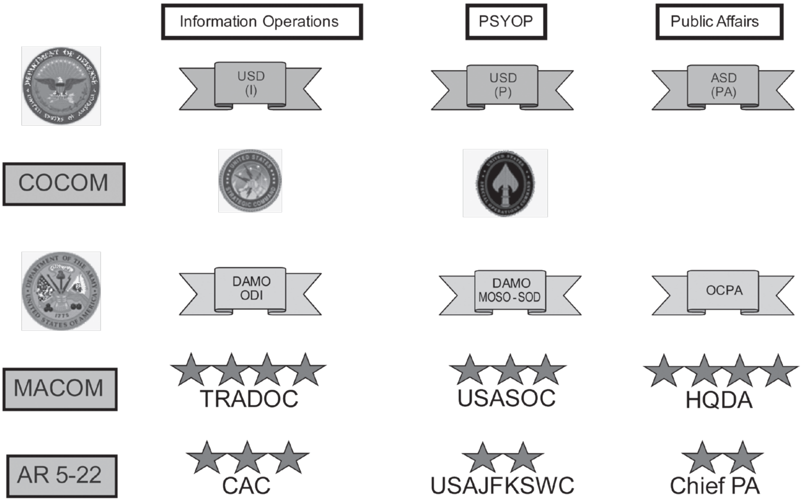


Figure 1

Prior to splitting PSYOP forces along component lines, most agreed correctly that PSYOP functions would no longer be known as Special Operations Forces (SOF) functions, likely because most of the capability would lie in and is needed in the conventional force, but the proponent office remains in USSOCOM.[26]

The need for full-time, skilled professionals to plan influence activities has only increased since 9/11. But active component brigades and divisions must rely on the IO proponent and IO trained officers to fill a void created by the lack of available PSYOP officers and a PSYOP proponent office that falls in USSOCOM. As a consequence, the Army has two functional areas, PSYOP and IO, which are increasingly confused or seen as redundant and two corresponding proponents that work at cross purposes.

Doctrinal Impediments to Coordinating Strategic Communication

The third issue is doctrinal inconsistencies with regard to the informational efforts – PSYOP, IO, Public Affairs (PA) – of the military instrument of power. While these inconsistencies are admittedly minor in themselves, in the context of the legal and organizational problems above, the discrepancies are magnified and must be addressed. These conflicts have contributed to the lack of clear and vertically nested strategic messages and the absence of coordination between IO, PA, and PSYOP at the tactical and operational levels. A side-by-side comparison of IO and PSYOP doctrine shows a contradiction in how the staff elements see themselves working together.

Army Field Manual (FM) 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures makes the claim that coordinating PSYOP is the responsibility of the IO officer: "Once PSYOP tasks are determined, the PSYOP officer coordinates them with higher headquarters for the G-7….The G-7 exercises coordinating staff responsibility over the PSYOP officer."[27] This clarity is muddled somewhat by the PSYOP community, which has a history of and preference for working under a unit's operations officer. *FM 3-05.30 Psychological Operations* by contrast maintains "A [PSYOP Support Element] normally works for a supported force S-3, G-3, or J-3…"

In 2007, *FM 3-05.301 PSYOP TTP* added G-7 to the list of possible bosses, but PSYOP doctrine continues to minimize its relation to IO.[28] Recently published, *FM 3-0 Operations* attempts to clarify the relationship between PSYOP and IO, by making PSYOP one of the capabilities of the information engagement task.[29] But it also leaves enough room to keep the dispute alive by noting that commander "may integrate [PSYOP] capabilities into the operations process through information engagement *and the targeting process* [my emphasis]," adding "Psychological operations units may also be task-organized with maneuver forces."[30] In discussing information tasks outside of the IO officer's responsibility, FM 3-0 continues to suggest that PSYOP can often fall outside the realm of information engagement and the IO officer, maintaining that "although command and control warfare is primarily accomplished with physical and tactical means, psychological operations and military deception activities can also provide important support."[31] Such distinctions would not be worth mentioning if PSYOP did not have a proponent outside the Army and a history of setting itself apart from conventional forces. Without a disinterested party capable of and willing to deconflict these contradictions, they will continue to be impediments to a coordinated message.

Recommendations

In order to better exercise the information instrument of power and achieve a unified strategic message, several changes need to be made throughout the USG and its departments. The first step is to modify the Smith Mundt Act and other legislation to clarify the requirement to effectively engage foreign audiences. This new legislation should include the recognition that regular and coordinated communication with foreign populations in every medium is necessary to advancing national objectives. Such programs must include foreign broadcasts, libraries, exchange programs, Internet engagements, and a diplomat corps trained in public diplomacy. These programs must be both factual and credible; they must take a strategic view, and they must be well funded, recognizing that only with heavy, repeat engagements over the long term and through numerous media can the U.S. message be received and processed. The new legislation should prohibit these programs from directly targeting a U.S. domestic audience, while simultaneously making it clear that these overt communications will inevitably be accessible to all publics in an interconnected world. And in the interest of keeping the American public informed, it is imperative that such information be made available to interested parties on request. Only by maintaining a high degree of transparency in the goals and processes of Strategic Communication programs will lawmakers and the American public be able to support their government's tactics.

The U.S. Strategic Communication effort also requires leadership from the White House, synchronization across organizations, and a corresponding reorganization of and within agencies and departments. And there must be acknowledgement that Strategic Communication is a long term effort not driven by crises. At the highest levels a single office reporting to the National Security Council needs to develop and approve themes for the entirety of the government. Themes and supporting messages must then be developed further by a single organization – a revitalized and enlarged USIA – with an ability to integrate into any government agency seeking to communicate with a foreign audience. Within each department, reorganization must allow for coordination with USIA personnel and facilitate internal coordination of influence activities. This is particularly important in the DoD, where PSYOP forces need to be removed from USSOCOM and viewed as elemental to conventional operations at every level. Similarly, the PSYOP proponent office should be placed within the Army's Training and Doctrine Command and integrated with the IO proponent. Public Affairs too, must be integrated with this proponent. The responsibility within DoD for coordination of global Strategic Communication should then be assigned to a single functional command and overseen by a single Assistant Secretary of Defense. Domestic messaging would then be coordinated within the DoD and synchronized with the national Strategic Communication plan.

Finally, DoD organizational changes must also be reflected in supporting doctrine. Within the Army, the need for a separate IO officer (S/G-7) outside of and distinct from the operations section should once again be revisited. If the information battle is critical in the current operational environment, it will often be the primary focus of unit planners. The Army information capabilities must be integrated with all unit plans and operations, they must support a message nested into the Strategic Communication plan, and Army communication professionals must have access to trained USIA officers. These legal, organizational, and doctrinal changes would go a long way toward achieving a unified national message.

Improving the United States' Strategic Communication Strategy

Colonel Robert H. Risberg
United States Army

America's image in the world is faltering. Recent surveys find that majorities in 10 of 15 countries polled do not trust the United States, that half of people surveyed in 25 nations think the U.S. plays a negative role in the world, that majorities in five Middle East countries have lowering opinions of the United States, and that the opinion of foreigners, particularly Europeans, toward Americans has substantially declined since 2002.[1] Why is this the case and, more importantly, how can the United States regain its once held position of popularity among the peoples of the world?

There are many reasons for America's falling global public opinion numbers. Some of it can be blamed on the natural resentment of people to the "richest country on earth," the "biggest consumer nation in the world," and to the sole superpower who dabbles its fingers in every corner of the globe. Much of this decline in international public standing is the result of unpopular wars in Afghanistan and Iraq. The United States is viewed as invading sovereign nations, on an anti-Muslim crusade, and causing much human suffering. While these reasons may explain the surface causes of American unpopularity around the world, they do not address the root cause of the symptoms of envy, resentment, and fear of the United States that seems indicated by the surveys and polls.

Americans rightly see the United States as a force for good in the world. No nation in history has been as generous to those in need, as forgiving of past enemies, or as unselfish as the United States. After all, it is America that comes to the aid of people stricken by natural disaster. It is America that offers the dream of success and prosperity for anyone willing to work for it. It is America whose soldiers have fought and died in foreign lands not for the purpose of conquest, but for the purpose of liberation from tyranny and oppression. Why is this view of

America not shared by the majority of people around the world at the beginning of the 21st century?

A major part of the answer to this question is the failure of the United States Government (USG) to effectively use strategic communication to inform and influence populations, foreign and domestic, to recognize the value of American efforts around the world, to understand and support American foreign policy objectives in the war on terror, and to recognize our broad contributions to development of the global society. In the early part of the 20th century, America was respected as the fresh, young nation stepping in to help the old powers resolve the disputes that brought war to Asia and to Europe. In the middle part of that century, the world was grateful for America as it led the effort to stop the tyranny of fascism from dominating the world. During the Cold War, America was seen as the bulwark of freedom against the spread of oppressive communism. Today, America leads the fight against rogue states, international terrorists, and religious extremists who willingly slaughter innocent civilians in pursuit of political and cultural agendas. Unfortunately, much of the world resents and fears the United States because they do not understand American objectives and receive a distorted and negative view of American actions through propaganda, manipulated news, and America's own tunnel-visioned overreliance on the military aspect of national power.

This paper will review the current USG strategy for using strategic communication in the war on terror, discuss the weaknesses and shortfalls of that strategy, and recommend specific actions to strengthen the strategy and improve its effectiveness.

U.S. Strategic Communication Strategy

As the War on Terror unfolded after 2001, the USG recognized the need to improve its use of information as an element of national power, often called strategic communication. American officials recognized the lack of international popular support for U.S. policies and actions and correctly attributed much of the blame to a failure in strategic communication. At the same time, America's enemies have proven to be very adept at leveraging the information environment. Al Qaeda attempts to manipulate nations with messages delivered via Internet postings, videos smuggled out of caves, and the televised images of bombs exploding in crowded public places (ask the losers of the Spanish parliamentary elections in 2004). As Dennis Murphy and James White point out in their recent article, *Propaganda: Can a Word Decide a War?*, propaganda is the weapon of the insurgent cell, "It costs little, is easy to distribute, and has near-immediate worldwide impact. The improvised explosive devices that have killed and maimed so many U.S. troops in Iraq are propaganda weapons. Their impact is not the tactical kinetic victory, but the strategic propaganda victory."[2] Hezbollah's use of aggressive strategic propaganda effects in its 2006 conflict with Israel took what started out as a justified, internationally supported strategic victory for Israel (defending herself from terrorist rocket attacks) and turned it into a strategic defeat. The bombing of Iraq's Al-Askari Shiite mosque in February 2006, in order to fuel sectarian strife and violence, is an example of tactical operations supporting an information strategy.[3]

In May 2007, the USG published the *National Strategy for Public Diplomacy and Strategic Communication*. This new strategy document resulted from recognition by the Bush administration that the U.S. needed an integration plan for its new emphasis on strategic communication. The plan was based on recommendations from more than 30 different studies of U.S. policy, feedback from across the USG interagency, academic institutions, and public relations professionals in the private sector.[4] Then Under Secretary of State for Public Diplomacy and Public Affairs, Karen Hughes, said "the plan is designed to provide unified strategic framework for U.S. government communications, yet be flexible and adaptable to meet the different needs and responsibilities of very diverse government agencies."[5]

The strategy establishes "three strategic objectives to govern America's public diplomacy and strategic communication with foreign audiences: 1) America must offer a positive vision of hope and opportunity that is rooted in our most basic values. 2) With our partners, we seek to isolate and marginalize violent extremists who threaten the freedom and peace sought by civilized people of every nation, culture and faith. 3) America must work to nurture common interests and values between Americans and peoples of different countries, cultures and faiths across the world."[6] It goes on to define the strategic audiences (key influencers, vulnerable populations, and mass audiences)[7] and establish public diplomacy priorities (expand education and exchange programs, modernize communications, and promote the "diplomacy of deeds").[8] The strategy calls for specific interagency coordination structures (a Counterterrorism Communications Center within the Department of State, an Interagency Crisis Communication Team, and regular monitoring of implementation) and addresses actions required by each agency and embassy in their role in public diplomacy and global communication, as well as identifying the need for increased funding to resource all of these efforts.[9]

This new strategy was designed to tie together all of the strategic communication initiatives being undertaken by various agencies of the USG, many of which were uncoordinated, that attempted to fill the need being realized more and more as the war on terror progressed. The 2002 *National Security Strategy* identified the need for "a different and more comprehensive approach to public information efforts that can help people around the world learn about and understand America."[10]

In the fall of 2001, the Department of Defense (DoD) had established the Office of Strategic Influence (OSI) to be the central coordinating agent for "a strategic information campaign in support of the war on terrorism."[11] This effort produced little and in February 2002, the Secretary of Defense dissolved the office due to opposition from government public affairs officials who feared it would undermine their credibility, and from negative U.S. and international media coverage alleging the office intended to place lies and disinformation in foreign news media.[12]

In 2002, the National Security Council (NSC) created the Policy Coordination Committee (PCC) on Strategic Communication. This PCC included members from across the interagency and was chaired by the Under Secretary of State for Public Diplomacy and Public Affairs. Its mission was "to develop and disseminate the President's message around the world by coordinating support for international broadcasting, foreign information programs, and public diplomacy; and to promote and develop a strategic communications capacity throughout the government."[13]

In early 2003, The Bush administration formed the Office of Global Communication (OGC) within the White House in order to establish coordination across the interagency on informational matters. This office was to be an adviser to the President, the executive department and agency heads on the "utilization of the most effective means for the USG to ensure consistency in messages that would promote the interests of the United States abroad, prevent misunderstanding, build support for and among coalition partners of the United States, and inform international audiences."[14] Unfortunately, the OGC was not effective in this mission and it was closed in 2005 as the administration shifted responsibility for strategic communication efforts to the Office of Public Diplomacy and Public Affairs in the Department of State (DoS).

In addition to creating new organizations to handle various aspects of USG strategic communication efforts, some no longer functioning, the DoD and DoS have led the way within the interagency to engage in the process of developing new doctrine and guiding concepts that will make strategic communication an important part of ongoing operations and planning. Each agency is preparing an agency-specific strategic communications plan that will nest within the overall national strategy.[15]

Assessing the U.S. Strategic Communication Strategy

Is the U.S. national strategy for strategic communication working? There is no doubt that the senior officials of the Bush administration "get" the need for effective strategic communication efforts to support American policy. Officials from DoD, DoS, the White House, and Congress have all acknowledged the need for action on improving American strategic communication efforts and have backed up those acknowledgements with actions. Progress is being made, but is the strategy set up for success?

In testimony before Congress in the spring of 2007, then Under Secretary Hughes said, "Public diplomacy now has a place at the most senior policy tables of our government; our public diplomacy programs are reaching more people around the world more strategically than ever before, and public diplomacy is now viewed as the national security priority that it is."[16] She went on to cite several examples of improvements in USG public diplomacy actions, including yearly increases in the number of student and exchange visitor visas issued, expanded partnering with American colleges and universities to attract foreign students to U.S. schools, expanded English language teaching programs for young people in foreign countries, creation of a Rapid Response Unit that monitors international news media and produces daily reports for American policymakers on world news as well as emailing thousands of foreign officials the U.S. position on issues mentioned in international news stories, the establishment of high tech digital outreach teams that work to counter misinformation and myths on Arabic Internet blogs, making public diplomacy part of the criteria used to evaluate all American ambassadors and foreign service officers, and expanded outreach to the private sector for foreign disaster relief assistance and education and training programs.[17]

Other evidence of progress can be seen in new efforts to recruit successful Muslim-Americans from the private sector to speak to foreign Muslim audiences about the United States, new guidelines to American diplomats and other officials serving abroad that require them to seek out and engage foreign media outlets in order to explain American policies and views, and the creation of DoS communication hubs in London, Dubai, and Brussels (more were established in 2008) that have the mission of actively engaging foreign news media to present American views and comments on important policy topics.[18]

Clearly, progress has been made over the last few years as more emphasis has been placed on informational power and strategic communication, but critical weakness and shortfalls still exist. Is there an Ends-Ways-Means mismatch for the American strategic communication strategy? Current evidence says yes.

In terms of the *Ends* for the U.S. strategic communication strategy, the national strategy document listed the three strategic objectives presented previously in this document, but not in sufficient detail to effectively guide policy formulation or the planning and execution of strategic communication efforts. While the strategy makes clear America's goals of "offering a positive vision of hope and opportunity," to "isolate and marginalize violent extremists," and to "nurture common interests and values," it does not provide a good framework for organizing and executing American strategic communication efforts.

One of the first problems with USG strategic communication efforts is the lack of a single, common definition for strategic communication. The DoS sees strategic communication as primarily public diplomacy and public affairs activities. In the 2006 *Quadrennial Defense Review*, the DoD defined it as "focused U.S. Government processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs and actions synchronized with other elements of national power."[19] The NSC defines it as "the coordination of statecraft, public affairs, public diplomacy, information operations, and other activities, reinforced by political, economic, and military actions, in a synchronized and coordinated manner."[20] Various think tanks define strategic communication as the aggregation of methods used by the Departments of State and Defense to deliver strategic effects,[21] or express it in terms of *Ends* (cognitive information effects on attitudes and perceptions leading to changes in behavior), *Ways* (strategic communication), and *Means* (integrated words, images, and actions),[22] or that "strategic communication means persuading allies and friends to stand with you. It means persuading neutrals to come over to your side or at least stay neutral. In the best of all worlds, it means persuading adversaries that you have the power and the will to prevail over them."[23] The Defense Science Board (DSB) described strategic communication as an instrument governments use to understand global audiences and cultures, engage in a dialogue of ideas between people and institutions, advise policymakers, diplomats and military leaders on the public implications of policy choices, and influence attitudes and behavior through communication strategies.[24] Even though there is no common definition for strategic communication in the USG, there are some common threads among the various definitions. These common threads indicate that strategic communication includes public diplomacy, public affairs, and information operations designed to inform and influence people using messages tailored to specific audiences, messages designed to promote the appealing values of America, and the coordinated use of words, images, and actions to get these messages to their intended receivers. What most officials seem to mean by the term strategic communication is the effective exercise of the informational instrument of national power – the big **I** in the strategic thinkers' acronym of **DIME** (Diplomatic, Informational, Military, and Economic instruments of national power). As defined by Robert Neilson and Daniel Kuehl, the information element of national power is the "use of information content and technology as strategic instruments to shape fundamental political, economic, military, and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[25] To date, no single definition of strategic communication, incorporating these key aspects, is in use across the government.

Another major issue with the *Ends* of the U.S. strategic communication strategy is that there has been no single, consistent theme underlying all USG strategic communication efforts in support of the war on terror. Indeed Americans, and the entire world, have received mixed messages about why the United States is fighting a war on terror and what the basic strategy is for winning that war. President Bush and other officials of his administration have not effectively provided a clear narrative that unites the majority of Americans behind a strategy for victory in the way the mostly consistent narrative, supported by fairly consistent policy goals, kept the public behind the strategy of containment of the Soviet Union and communism during the Cold War. Not only has the Bush administration confused the public with alternating focuses on weapons of mass destruction, the spread of democracy, and transnational terrorist groups, but the President's political opponents, for short-term political gain, have sown doubt and suspicion among the American people and foreign audiences with declarations of defeat in Iraq and calls for unconditional withdrawal of American troops from the combat theaters. Near historically low approval ratings for the President's policies demonstrate some of the result of the failure to have a clear narrative underlying strategic communication efforts on the war on terror. As Joel Roberts points out in his paper on the battle of ideas, "this decrease in support is not a result or indication of a lack of patriotism within the country, but due to the administration's paucity of internal strategic communication themes to continually remind the public of the cause and continued need for the war. We do not provide a clear strategic message to the American people concerning the overall War on Terrorism; particularly how the operations in Iraq and Afghanistan are a part of a larger campaign."[26]

In terms of the *Ways* of the U.S. strategic communication strategy, several weaknesses appear. The key problem is integrating strategic communication efforts across the USG interagency. The Under Secretary of State for Public Diplomacy and Public Affairs, the USG official rhetorically charged with coordinating all strategic communication efforts, has no authority over the public diplomacy functions or personnel working public diplomacy or public affairs functions outside the Office for Public Diplomacy and Public Affairs in DoS, and has little say over resources devoted to public diplomacy.[27] This problem was identified by the DSB in 2004 and remains an issue.[28] This problem is compounded by the fact that the Strategic Communication Policy Coordination Committee within the NSC, chaired by the above mentioned Under Secretary, has no authority to task and/or direct agencies of the government.[29] The broader issue is that the USG still does not have a single entity charged with developing, coordinating, executing, training for, and resourcing strategic communication efforts for the Nation.

Having a single government agency responsible for USG communication efforts is not new. When the United States entered World War I in April 1917, government and military leaders saw the need to coordinate USG information efforts. In response, the government established the Committee on Public Information, also called the Creel Committee.[30] Similarly, during World War II the United States created the Office of War Information (OWI) that worked to generate media coverage for both domestic and foreign audiences on the progress of the war effort, using services like the Voice of America radio network.[31] When the Cold War heated up in the early 1950s, the United States formed the United States Information Agency (USIA) to confront the Soviet Union on the information battlefield. President Kennedy described the role of the USIA as, "to help achieve U.S. foreign policy objectives by (a) influencing public attitudes in other nations, and (b) advising the President, his representatives abroad, and the various departments and agencies of the implications of foreign opinion for present and contemplated U.S. policies, programs, and official statements."[32] During the Cold War, public diplomacy initiatives and international broadcasting helped contain and defeat Communism, promote democracy, explain American foreign policy, and expose foreign audiences to American values.[33] The USG does not have a single agency or entity leading, coordinating, and executing strategic communication efforts today.

Various recommendations exist for what a strategic communication agency should look. In 2004, the DSB recommended the formation of "an independent, non-profit and non-partisan Center for Strategic Communication to support the NSC and the departments and organizations represented on its Strategic Communication Committee" that is modeled on federally-funded research and development centers like the Rand Corporation.[34] Writing in the DISAM Journal, Curtis Jenkins calls for establishing a "Joint Inter-Agency Task Force for Strategic Communication" including representatives from the DoS, DoD, Department of Justice, Central Intelligence Agency (CIA), Department of Homeland Security, and the NSC as a minimum, with the President as the head of the task force.[35] Each of these recommendations has merit, but the most effective way of maximizing the integration, coordination, and resourcing of strategic communication efforts across the entire USG is to establish a cabinet-level agency whose head holds equal status to the Secretaries of State and Defense and who sits on the NSC.

As Bruce Gregory points out, real improvement in USG strategic communication efforts requires more than just reform of "coordinating" processes, but requires processes that provide "strategic direction" for all USG efforts.[36] This is best achieved by having a single agency that can translate the President's guidance into this strategic direction.

Unfortunately, effective in 1999, the USIA was abolished, with most of its functions absorbed by the DoS.[37] This move was part of the general downsizing of America's national security apparatus in the wake of the end of the Cold War. It also followed up on some of the key recommendations of the 1975 "Stanton Commission" which recommended abolishing the USIA and replacing it with a new quasiindependent Information and Cultural Affairs Agency which would combine the cultural and educational programs of the USIA and DoS, the establishment of a new Office of Policy Information within DoS to administer all programs that explain U.S. foreign policy, and the setting up of Voice of America as an independent federal agency under its own board of governors.[38] A result of folding USIA functions into the DoS and making the Voice of America and other USG broadcasting programs independent, is that now the National Endowment for Democracy, the DoS, and the United States Agency for International Development (USAID) are all in the business of running programs in the areas of education reform, political reform, state-building, civil society, and democratization, while interagency mechanisms for coordinating these programs remain weak or non-existent.[39] Some researchers also point to the organizational culture of the DoS as part of the reason why the merging of USIA functions into State has not produced effective strategic communication efforts. Carnes Lord, a former USIA and NSC official and former national security assistant to Vice President Quale, says that "the information function has always lacked prestige within the culture of the Foreign Service, and is currently ghettoized (that is public diplomacy is a fifth career cone within the Foreign Service, distinct from the prestigious political cone). This has meant consistent undermanning and underfunding of public diplomacy activities."[40]

Also a *Ways* shortfall, and working to confuse and slow effective strategic communication efforts by the USG, are the antiquated laws and regulations restricting government action in regard to information use. Due to perceived excesses by the OWI during World War II, and due to a general public distrust and dislike of anything possibly falling into the category of "propaganda," the Congress has placed restrictions and prohibitions on the dissemination within the United States of informational products intended for foreign audiences. In 1948, Congress passed the Smith-Mundt Act which, although recognizing the importance of marshalling American cultural and information outreach efforts in support of national engagement in the Cold War, carefully stipulated that these programs intended for foreign audiences could not be disseminated in the United States.[41] Restrictions like those of the Smith-Mundt Act and others, are not only relics of the Cold War and of a different type of conflict, but also do not reflect today's state of technology in which information flows almost instantaneously around the world on satellite TV, digital cellular networks, and the Internet. It is unrealistic to assume that information intended for foreign audiences will not quickly make its way to American audiences and vice-versa.

Another major *Ways* weakness is the common use of strategic communication as an "afterthought" in the policymaking and strategic planning process. U.S. Government processes typically treat strategic communication as a supporting element to the primary operation or policy effort, as often evidenced by the strategic communication portion of a policy or plan being relegated to an annex or appendix to the main document. Similarly, the establishment of a separate Strategic Communication Policy Coordination Committee on the NSC implies that strategic communication is a separate function.

Strategic communication and informational themes, messages, options, and approaches must be included from the beginning of policy formation and campaign planning. The idea of involving strategic communication specialists and planners early in the policy formulation process is not new. Richard Halloran illustrates this well when he recounts famed journalist Edward R. Murrow's response to President Kennedy's request that he head the USIA in 1961, "If you want me to be there on the crash-landings, I better be there on the takeoff."[42] According to an experienced strategic communication practitioner, a good analogy for this early involvement in the planning process is that of marketing versus advertising. Advertising is figuring out how to sell a product after the product is already developed while marketing is figuring out what the potential customers want, how best to design the product to meet the need of the customers, and how best to present the product to the customers that will get them to buy it.[43] Larry DiRita, an aide to then Secretary of Defense Donald Rumsfeld, put it this way, "the old fashioned idea that you develop the policy and then pitch it over the transom to the communicator is over. You're continually thinking about communications through the course of the policy development process. The policy gets better when it's subjected to the rigors of knowing how you're going to communicate that policy."[44] The current war on terror, and the predominant form of warfare most experts foresee in the 21st century, is what Thomas Hammes calls a

Fourth Generation War (4GW)in which America's adversaries rely less on direct military confrontation in the conventional sense and more on irregular warfare with information operations and attacks designed to further an informational theme or message.[45] As Hammes describes a 4GW campaign, the planner "must determine the messages he wants to send, the networks available to him, the types of messages those networks are best suited to carry, the action that will cause the network to send the message, and the feedback system that will tell him if the message is being received."[46] This approach should be at the heart of all policy formulation and strategic campaign design.

Part of this formalization of strategic communication into all USG and U.S. military planning processes must include processes and plans that anticipate mistakes and failures, as well as processes and plans for seizing opportunities in the informational realm. No one gets everything right and no plan or policy works perfectly. Planners and policymakers can anticipate mistakes or failures and have already thought through options for using strategic communication means to mitigate those things that don't go well. Similarly, planners and policymakers must expect that situations will arise that will present opportunities to further informational themes, goals, or objectives. Processes must exist that facilitate rapid seizure of these opportunities.

Finally, one of the most important *Ways* shortfalls of the U.S. strategic communication strategy is the failure to adequately address what Linton Wells calls "strategic listening." Wells correctly claims that it is not enough just to deliver the message. Successful long-term strategic communication must have listening and influence analysis as critical prerequisites. He concludes that effective strategic listening includes: receiving without judgment (seeing what's there, adapting, and finding ways to connect); being willing to relinquish control, moving from strongly held positions, and co-creating; making use of user-generated content; and sustaining involvement in an area (taking a long-term focus and maintaining contact despite the agenda of the moment).[47] Effective strategic listening will not only aid in presenting U.S. policies and actions in the best ways to the right audiences, but will also aid in developing policies and taking actions that more effectively achieve the goals and objectives intended. This is another area best planned, trained for, and coordinated by a single lead strategic communication agency.

In the area of *Means* for the U.S. strategic communication strategy, some of the interagency coordination mechanisms called for in the strategic communication national strategy document have been established, but with limited effect. The Counterterrorism Communications Center is up and running within the DoS and includes representatives from the Departments of State and Defense, the CIA, and USAID. While this center is actively monitoring breaking news events related to terrorism, it lacks authorities to direct action, informational or physical, by any other parts of the government. Also, the Interagency Crisis Communications Team has yet to be formed and tested.[48]

Another major *Means* weakness is in the area of resources. While there is broad agreement within the USG that the United States needs "more strategic communication," real efforts are only being made by the DoD and DoS. The NSC has a PCC that is supposed to review and coordinate strategic communication policy formulation across the interagency, but its effectiveness is limited because agencies other than DoD and DoS do not have strategic communication personnel to work on the PCC.[49] Even within the two most prominent and forward leaning strategic communication agencies of the government, DoD and DoS, not everyone is aware of where they fit into the government's overall strategic communication strategy. For example, in November 2007, the head of the New York office of the DoS's Foreign Press Office did not know about the National Strategy for Public Diplomacy and Strategic Communication that had been published five months earlier.[50] Much of the problem is funding. The DoS was happy to receive $1.5 billion for Fiscal Year 2008 for strategic communication efforts, with almost half of that ($668 million) for broadcasting programs like the Voice of America. However, no other agency (with the exception of DoD) received funding specifically to address strategic communication programs, processes, or personnel.[51]

Another *Means* weakness hampering USG strategic communication efforts is the lack of integrated and coordinated research on foreign audiences. The General Accountability Office (GAO) reports that

"U.S. Government agencies conducting research on foreign audiences currently do not have systematic processes in place to assess end-user needs or satisfaction pertaining to research products, or to coordinate or share research," and that "efforts to coordinate and share audience research data are hampered by the lack of interagency protocols for sharing information, a dedicated forum to periodically bring key research staff together to discuss common concerns across all topics of interest, and a clearing house for collected research."[52] This is another area in which having a single agency responsible for coordinating all USG strategic communication efforts, including research and analysis on foreign audiences, would benefit American strategic communication efforts.

A further significant *Means* shortfall is the lack of effort to harness the power of the American media and entertainment industries in support of U.S. strategic communication efforts. Movies, television, music, and video games have tremendous influence over various populations and are extremely good mediums for sending messages. For good or for bad, American movies, television, and music reach every corner of the globe. Much of the world learns most of what it knows about America, about Americans, and about American policies from these sources. Movies and television especially can help to achieve some of the goals (offering a positive vision of hope and opportunity, isolating and marginalizing violent extremists, and nurturing common interests and values) of the U.S. strategic communication strategy.

As an example, a growing media for the influence of young people worldwide is video games. There are already video games developed by Arab companies that involve heroic young Arab men fighting Israelis and Americans. Couldn't similar games, distributed via free Internet downloads in the same manner as the U.S. Army recruiting video game, *America's Army*, show heroic Arab men battling al Qaeda and other extremist organizations with the aid of America? The DoS has made some efforts along this path recently when it worked with the Walt Disney Company to produce a seven minute film and hundreds of still images featuring American people from all regions and walks of life for showings in U.S. consular offices worldwide and in arrival areas of foreign flights into the United States.[53] While politically left-leaning Hollywood would probably not be receptive to direct USG involvement in movie making, there may very well be Hollywood producers, writers, directors, and actors who would respond to formal and informal encouragement to produce movies that honestly highlight American ideals of freedom, democracy, and respect for human rights and that are targeted to Muslim and other key audiences around the world.

Also in the area of *Means* is the relatively untapped resource of well-publicized, high-profile actions that highlight the many good things the United States does every year for people in need around the world. Under Secretary Hughes referred to the "Diplomacy of Deeds" as one of the keys to successful USG strategic communication.[54] One of those deeds cited by the Under Secretary and others were the recent humanitarian missions to South America by the U.S. hospital ship *Comfort* and Southeast Asia by her sister ship *Mercy*. These missions, in which the *Comfort* and *Mercy* provided much needed medical assistance to the people of those regions visited, improved public opinion of the United States in those areas.[55] The United States should seek out more opportunities like these and do a much better job of publicizing those actions. While there is no doubt that the people directly affected by one of the *Comfort* or *Mercy* visits have a better opinion of the United States, but how many other people in similar countries never heard a word about it?

An additional area of needed *Means* improvement is that of countering enemy propaganda and inaccurate or misleading (accidental or intentional) news reports and media portrayals of America, Americans, and American actions. Murphy and White accurately point out that "failure to quickly and accurately react to propaganda cedes the international information environment to the enemy. The reality of instant communications means that individuals on the ground at the lowest tactical level should be empowered to respond to propaganda to the best of their ability."[56] The DoS is making some efforts in this area with its Rapid Response Unit, foreign communication hubs, and digital outreach teams, but this effort is not government-wide. This task can fall primarily to rapid reaction teams or "truth squads" (like DoS's Rapid Response Unit) created within each USG agency and be coordinated by an expanded USIA-like information agency. Challenging adversary propaganda and inaccurate or slanted news stories with speed and consistency not only gets accurate information to the various audiences around the world, but also has the longer-term benefits of making propagandizing harder for the adversary and of making news organizations more careful and more balanced with their reporting. Journalists only have to be exposed in public as victims of propaganda or inaccurate or biased reporters a few times before they will police themselves.

Recommendations for Improving U.S. Strategic Communication for the War on Terror

While some parts of the U.S. strategic communication strategy for the war on terror are gaining traction, the USG should take additional steps and set additional processes in place to make the strategy more effective. The following recommendations use the Ends-Ways-Means framework to outline ideas for immediate action by USG senior policy makers.

In the area of *Ends* for the U.S. strategic communication strategy, the first step is to identify, develop, and promulgate a set of overarching principles that will govern and guide all of the USG's strategic communication efforts. These principles form the bedrock on which to build a successful strategic communication strategy for the war on terror, and must be included in a strategic communication vision statement issued by the President and followed by all parts of the Federal government. The three strategic objectives (ends) identified in the U.S. national strategic communication strategy document provide a good set of generic goals for American strategic communication efforts, but they do not provide enough detail to effectively guide the efforts of strategic policy and decision makers across the government. The basic principles of an effective strategy should include:

Strategic communication efforts are an interagency responsibility in which each agency has a part to play in planning, resourcing, and executing strategic communication activities in support of American foreign policy objectives.

Strategic communication efforts are focused on the long-term success of American foreign policy in securing the homeland, protecting vital U.S. and allied interests around the world, and in promoting regional stability and the spread of democratic ideals and institutions. United States policy, plans, and actions must support a long-term commitment to the people, institutions, and resources vital to peaceful prosperity for all members of the family of nations.

Strategic communication is embedded into the basic processes used for all policy formulation and campaign planning, and is resourced as a top priority of each USG agency.

Successful strategic communication efforts must include processes and procedures for strategic listening and learning from other nations, organizations, and people, and all strategic policies and campaigns must convey the willingness of the United States to consult with, cooperate with, and learn from allies and partners.

The United States will not be universally loved and welcomed around the world, but all people – friends and foes alike – must see it as consistent, fair, determined, generous, agile, and willing to act and engage. There is natural resentment to the richest nation on earth, the great consumer nation, and the unchallenged superpower, but America has a unique responsibility to represent what is right about civilized people. Remember Ronald Reagan's advice, it is nice to be liked, but better to be respected.

With these guiding principles in mind, the following set of 10 specific actions fall into the Ends-Ways-Means areas for improving the USG's strategic communication strategy:

- ***(End) Develop a single overarching "narrative" for the War on Terror from which all strategic communication efforts flow.*** Counterinsurgency expert David Kilcullen talks about the need for a "narrative" or consistent, coherent message that ties strategic communication themes together. He says people are not mobilized individually by a cold consideration of rational facts, but are mobilized in groups by influences and opinion leaders, through a "cultural narrative" that include seven basic elements: a simple, easily expressed explanation for events; a choice of words and story format that resonates with the target group; symbolic imagery that creates an emotional bond; elements of myth that tap into deep cultural undercurrents of identity and appeal to universal ideals; a call to action; credibility built on a high degree of consistency between what is said, what is done, and what is seen; and a future focus that inspires people to mortgage current self-interest for future benefits.[57] The specific messages (using words, images, and actions) sent out as a part of strategic communication campaigns must be tailored to the audiences for which they are intended, but there must be one overarching, consistent narrative that underlies those messages.

- ***(Ways) Create an independent federal agency responsible for directing, coordinating, and executing strategic communication for the U.S. Government.*** This agency should have equal standing with the other major departments of the government and its head should be an equal member of the President's cabinet. The head of this agency should sit on the NSC and the Homeland Security Council to directly advise the President. It should have the authority to task and direct in support of public diplomacy, public affairs, and other informational activities. It should be responsible for media analysis, foreign public opinion analysis, and other analysis (all of the things related to "strategic listening" as described earlier) to support themes, messages, and actions. This agency should be responsible for training communication specialists and public affairs officers for the U.S. Government. This agency should also be non-political and non-partisan in the manner of the FBI, CIA, and Federal Reserve. It should run all U.S. international broadcasting efforts and take over the cultural exchange programs, educational programs, and democracy promotion programs currently under the DoS and other agencies.

- ***(Ways) Give the Under Secretary of State for Public Diplomacy and Public Affairs authority over and responsibility for all public diplomacy and public affairs functions of the DoS worldwide, to***

include the communication specialists and public affairs officers serving in embassies around the world. If this Under Secretary is to truly lead DoS's, and, as currently designed, the entire interagency, strategic communication efforts, he or she must have the authority to task and direct actions, to set priorities, and to determine how to invest resources.

- ***(Ways) Draft new legislation for Congressional action and executive agency regulations and orders that clarify strategic communication responsibilities, definitions, and limitations.*** The President should work with the Congress to pass new laws that will provide a common definition of strategic communication for the USG, that will take into account the current and emerging technologies that impact how and when audiences around the world receive news and information, and that facilitate the legitimate efforts of government agencies to inform and influence both American and foreign audiences. National leaders must admit that the United States actually does want to truthfully influence foreign audiences and that this cannot be done without simultaneously influencing American audiences. Informing people about the true nature and objectives of American foreign policy and influencing people to support those policies is not dishonest and can absolutely be done without misleading the public.

- ***(Ways) Create policy development processes and campaign plan development processes that formalize mechanisms for strategic communication of specific messages at their heart.*** All policy formulation and strategic campaign design processes should have strategic communication aspects, messages, and actions as part of the base plan rather than as an appendix or afterthought.

- ***(Means) Fully resource the Strategic Communication strategy with people, training, and funds.*** The President should request, and Congress should appropriate, funds for each USG agency specifically targeted to conducting strategic communication. Each agency needs to hire strategic communication specialists. Strategic communication cannot be an additional duty for an already heavily tasked official. Congress should also specifically appropriate funds to support training programs for strategic communication specialists and should use its oversight responsibilities to require the heads of government agencies to periodically report their strategic communication efforts.

- ***(Means) Recruit the entertainment industry to help spread the message of what is good about America and what is bad about the extremists and terrorists.*** Movies, television, and music can highlight American ideals of freedom and human dignity and show the evils of extreme ideologies. Video games targeted to specific audiences in the Islamic world which reinforce good and demonize extremists, could be effective.

- ***(Means) Seek out and exploit opportunities for simple, yet meaningful American humanitarian assistance in the Muslim world.*** The United States does much good in the world that literally saves lives every year. These efforts should be expanded and publicized.

- ***(Means) Aggressively challenge adversary propaganda and inaccurate, misleading, and slanted news media reporting.*** U.S. Government officials from the highest levels down to the foot soldiers of each agency should review media reports about USG, American industry, U.S. military, and adversary actions to identify the mistakes, inaccuracies, and misleading news stories. Once identified, aggressively challenge those items and provide accurate information to correct the reporting and expose propaganda and biased media.

- ***(Means) Use communication planning techniques and the best communication planners from private industry and advertising firms to assist in strategic policy formulation and strategic campaign design.*** Communications planning is a technique developed in Europe and involves determining which media outlets and messages will work best for a particular brand. Over the last five years, several companies in the United States have put communications planning at the forefront of their thinking about how to better engage consumers.[58] Not only should the USG use this same technique to make its strategic communication more effective, but it should hire some of the same communications professionals who are making this work for private industry. The expertise exists in the private sector and there is no reason why the government should not harness this resource for the good of U.S. foreign policy and ultimately for the good of the nation.

Conclusion

After a slow start, the USG has realized the importance of effective strategic communication in support of U.S. foreign policy and the war on terror. The new strategic communication national strategy is slowly bringing more synchronization and integration to USG efforts at public diplomacy and strategic communication. More work needs to be done and implementing the recommendations laid out previously will help correct the current ends-ways-means mismatch in the strategy and ultimately make this strategy more successful.

The lessons of the wars in Iraq and Afghanistan, and those in the greater war on terror, have brought a new realization that America's great military power is not enough to achieve success in the conflicts of the 21st century. All elements of national power must be applied to the problems and challenges the United States faces in its role as the sole superpower in the world. These lessons, some reminiscent of those learned in earlier periods of conflict, are driving a substantial investment in strategic communication efforts by the USG. With some new guiding principles, new and expanded government structures and processes, and adequate resources, the United States can achieve its policy objectives and regain the respect and support of most the world.

Bridging the Cultural Communication Gap Between America and Its Army

Ms. Bobbie Galford
Department of the Army

Introduction: A Distinguished Past

For more than 232 years the United States Army has demonstrated a rich and proud heritage in defending America's homeland and serving U.S. national interests overseas. From the Revolutionary War to today's global war on terror, through peace and conflict, the Army has prevailed in the numerous missions it has conducted. American soldiers have achieved success throughout the years conducting worldwide operations such as humanitarian assistance, disaster relief, peacekeeping and nation-building while continuing to perform their primary warfighting role.

> *Our nonnegotiable contract with the American people is to fight and win the nation's wars. Every other task is subordinate to that commitment. To discharge our responsibilities to the nation, we maintain several core competencies. These are essential and enduring capabilities of our service. They encompass the full range of military operations across the spectrum of conflict, from sustained land dominance in wartime to supporting civil authorities during natural disasters and consequence management.*[1]

Through times of triumph and tragedy, the Army has been fortunate to have young men, and later women, of all segments of society fill its ranks in service to this nation. It is in large part because of these patriots, some of whom volunteered and others who were conscripted, many who served as career soldiers while others served only one tour of duty, that the United States stands today as the world's only military superpower. "To be ready for whatever comes in the future, if we are to remain the indispensable nation, we must have an effective and efficient military."[2] A strong Army will continue to play an integral role in the continued safety, well-being and success of our country.

Over the past decades, much of the American public has had a clear understanding of the U.S. Army and its purpose, values, roles and missions. This is due primarily to the personal relationships forged between U.S. soldiers and American citizens occurring throughout the United States. The Army is composed of a diverse mix of backgrounds representative of small towns to large cities in all regions of the country. It has provided a calling to Americans who have been both financially prosperous and poor and to college educated individuals as well as high school dropouts. And later in its history, the Army afforded opportunities to all ethnic groups and to both men and women who desired to serve. Until recently, almost everyone, in all segments of the American society, served with the Army or had a family member, educator, member of clergy, colleague or a friend join the Army's ranks either voluntarily or through a draft. Even during times when the American public disagreed with political decisions directly affecting the military or was disgraced by controversial events or actions involving Army troops, the vast majority of Americans still possessed a solid foundation and understanding of the need and reason for an Army. However, public attitudes toward the military since World War I have gradually eroded. "During both world wars the American public and media were extremely supportive of the military. In contrast, support was much less evident during the Korean War and, especially, during the Vietnam War. Yet, during the Cold War or late modern era, public attitudes were generally supportive of the military as an institution and of its budgetary demands, although there was some erosion of that support."[3]

Today the United States is a far different place. American culture, society and the Army as an institution have changed in response to a transforming world. As globalization evolved, the relationship between the public and the military changed and the communication gap between America and its Army widened. Two "overarching reasons" for this phenomenon are lack of military understanding by American elites because the Army has been a volunteer force for more than 30 years, and the establishment of a large peacetime military which has created a U.S. military garrison environment. This allowed the military to become self-contained and distinct from society.[4] "We need to reconnect with the American people," Major General John G. Meyers, former Chief of Army Public Affairs, said.[5]

A thorough examination of the culture of the United States Army and the trends and opinions of Americans no longer closely associated or linked with the Army is necessary to provide an analysis of how a lack of communication leads to misunderstanding, misinformation and apathy which, in turn, negatively affects Army recruitment, retention, funding and credibility. Tom Ricks, in his book, *Making of the Corps,* asserts that the gap between the military and the society it serves is made worse by the public's new ignorance of military affairs.[6]

In order to continue to have a strong, vital institution essential to maintaining America's future as a world power, the U.S. Army will be required to bridge the cultural communication gap between America and its Army. To effectively bridge this crevasse, the Army will need, at a minimum, to understand the primary issues creating the gap and then develop and execute varied strategic communication initiatives to close it. "Vitally important, strategic communication means persuading the nation's citizens to support the policies of their leaders so that a national will is forged to accomplish national objectives."[7] Achieving this goal will require Army leadership to continue to engage the American public, but to do so in different, creative and innovative ways. Programs and projects deemed effective today in meeting the Army's communication challenges should be continued and improved, but our leaders must continually think more strategically and creatively to develop future communication methodologies that are effective and timely. Since military effectiveness is improved by an Army supported by its wider society,[8] the U.S. Army will need the continued moral support, funding, and human capital of the nation to remain relevant.

The American public's lack of knowledge and awareness about the Army and general apathy toward our soldiers can be examined through the study of the potential future force, the composition of the current Army, the limited political and business elite association and involvement with the military, and the changing roles and missions of the United States Army.

Responsibilities and Challenges

The U.S. Constitution directs Congress to raise and support an army. Subsequently, Title 10 of the U.S. Code gives the Army the responsibility to organize, train and equip. The Army provides trained forces to the Combatant Commanders for use as they see fit. The United States discontinued using the draft to fill the ranks of its military services in 1972. Since that time, the Army has relied on recruiting an all-volunteer force. In the *2007 Posture Statement*, the Army lists "growing the all-volunteer force to sustain the long war" as one of its "core objectives which the Army must achieve."[9] The Posture Statement goes on to devote an addendum to the recruitment and retention of the all-volunteer force, stating that sustaining the all-volunteer force is a "fundamental strategic objective for the Army, that serves as a vital investment in the future security of our nation."[10]

Recruiting and sustaining an all-volunteer force is a critical task for the Army but continues to be a challenge for the U.S. Army Accessions Command. The first challenge is that of sheer numbers. American families today are smaller than ever before and, consequently, there are fewer youth. Only 3.35 million American's turned 18 in 1994; the lowest figure since 1964.[11] Increases in employment opportunities, improvements in the economy, more access to colleges and universities, and heightened negative public attitudes toward the global war on terror all hinder the number of individuals within the Army's primary recruiting market (17-24 year old males) interested in a tour or career with the U.S. Army. "Only about one in nine (11%) teens indicate that they have a "great deal" of interest in serving their country in a military capacity. Just 6% of girls say they have a great deal of interest in serving in the military, versus 15% of boys."[12] This target market, also known as Generation Y, has different norms, beliefs and aspirations than the recruiting target markets in the past. "They are more numerous, more affluent, better educated and more ethically diverse. More important, they are beginning to manifest a wide array of positive social habits that older Americans no longer associate with youth, including a new focus on teamwork, achievement, modesty and good conduct."[13]

It is essential that Army leadership strategically evaluate and grasp the culture of Generation Y in order to know what values and beliefs are important to potential recruits. According to a *Business Week* cover story Feb. 15, 1999, marketing to the members of Generation Y is an entirely new game. This group, born between 1979 and 1994 are 60 million strong and view life differently than those generations that came before them. They are pragmatic and respect and respond to truth, irony and humor. "Along with cynicism, Gen Y is marked by a distinctly practical world view, say marketing experts."[14]

Parental positive influence in a teen's decision to join the military has also eroded since U.S. involvement in the Second Persian Gulf War. A 2005 poll "asked Americans how they would react if they had a son or daughter who was planning to enter the military. Fifty-one percent say they would support that step, while 48% would suggest a different occupation. When the *Associated Press* asked the same question in 1999, 66% of Americans said they would support their child's decision, while only 29% would suggest their child try something else."[15]

Waning numbers of the Army's target market, a decrease in the propensity to enlist and the erosion of influencer support are not the only difficult issues recruiters face today. Many of those interested in serving in the U.S. Army simply are not qualified.

According the Army's *Posture Statement* only "45% of the primary recruiting market are potentially fully qualified or require a waiver, and only 29% are potentially fully qualified" for Army enlistment.[16] The Army competes with all of the other services in recruiting from this small group of candidates.

In addition to examining demographic trends used by the Army to recruit a new force, it is also helpful to study the tendencies and views of those already serving in the service in relation to retention. The attitudes and opinions of those currently serving, both in the enlisted and officer corps, have the ability to affect the relationship between the military and society, both positively and negatively.

"Almost 600,000 soldiers are on active duty today, (currently 507,000 in the active component, 46,000 in the Army National Guard and 28,000 in the Army Reserve). Over 40% (243,000) of them are deployed or forward stationed, serving in 76 countries worldwide."[17]

Many of these soldiers are serving on their second or third deployment tour and some have had their tours extended in support of the U.S. military strategy. In addition to being unhappy with increased and extended combat deployments, many of those in uniform are becoming increasingly critical of their military and political leadership and are more and more skeptical of the American public support for the troops in this war. "Many returning veterans have expressed doubts that the public supports their service and noted that the public does not have to make any sacrifice of its own. Any number of OIF [Operation Iraqi Freedom] vets have admitted a degree of annoyance that while they were serving overseas, the American people were out shopping."[18] Trust within the Army officer corps, especially between junior officers and their superiors, has led to a shortage of Army captains reflected by the number of officers leaving each year. "A recent *New York Times* article cited a young officer saying, 'Senior leaders will throw subordinates under the bus in a heartbeat to protect or advance their own career[s].'"[19] Soldiers are sharing their opinions with the public through the media, but more importantly with their decisions to leave the military service at the end of their tours.

According to recent U.S. census figures, the American population is now more diverse than anytime in history. "This is especially true for the labor force, where the influx of women and racial minorities represents one of the most profound changes in the American workforce in recent years. By 2025, the labor force is expected to be 48% women and 36% minority. In addition, there is increasing diversity among the college and college-bound population."[20]

Although the U.S. Army has made gains over the past several years in the recruitment of women and minorities, the organization's diversity is still not truly representative of American society. Although unrealistic to believe that half of the Army's troops will be female any time soon, it is essential that the Army continually evaluate opportunities within the service where women may be able to serve and open those positions to qualified females. Military occupational specialties currently closed to women, currently 9%, and constituting 30% of all active duty positions need to be routinely reviewed to determine if they really should be gender specific.[21]

Culture and Demographics

In several ways, the culture of the United States Army has evolved, transforming many of its previous beliefs and assumptions just as the culture of the rest of the nation has evolved. The U.S. Army has recognized and responded to the need for soldiers to be better educated, better trained, more technical, innovative, agile and flexible. "Perhaps because the Army has existed long enough to have been repeatedly, and sometimes brutally, forced to reexamine its role in national defense, self-reflection and analysis are vital components of Army culture," General Peter Schoomaker, former Army Chief of Staff, said. "We must be prepared to question everything in endorsing innovation and culture change in the Army."[22]

The changing and expanding role of the U.S. Army institution since the end of the Cold War has contributed to the lack of communication between the Army and society. The smaller, limited conflicts the United States has been involved in since the end of the Cold War required a changed Army that could deploy equipment and personnel rapidly to fight a different type of enemy. The capability necessary for the traditional role of land power assets is no longer the Army's focal point. The Army is transforming to meet the new world challenges, but those changes are occurring slowly and not without some angst and frustration throughout the organization. Transforming an entire institution, which involves changing doctrine, plans, equipment, training, structure and personnel to meet new requirements and multiple missions also requires organizational culture transformation that can lead to communication barriers. Understanding the organizational culture is essential to make effective and lasting change and to effectively communicate the changes, requirements and new roles and missions to both internal and external audiences.

Edgar Schein's model of organizational culture states, "Culture is not a single belief or assumption, it is a set of interrelated (but not necessarily consistent) beliefs and assumptions." Schein continues to explain that "the members of a culture hold values and conform to cultural norms because their underlying beliefs and assumptions nurture and support these norms and values."[23] John A. Nagl, in *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam,* defines organizational culture as a "persistent, patterned way of thinking about the central tasks of and human relationships within an organization."[24] If Army leadership concurs with these theories of culture, it is imperative for leadership to examine, evaluate, and understand the specific culture of the Army and to be prepared to reform the culture if necessary to maintain the health of the organization. Leaders need to comprehend core values, beliefs, assumptions and norms in order to influence the organization. They also need to understand the current culture and trends of our society in order better relate to the American public and to ensure the nation's youth consider the U.S. Army as both a viable employment option and an important and necessary defense entity.

Being a change agent, being prepared for turmoil and having the determination to see the change process through must be a personal priority for senior leadership. Leaders will need to demonstrate interpersonal, conceptual and technical skills to develop and implement the vision and strategies to sustain an innovative, agile and ethical army within a diverse, multicultural environment. Leaders will need charisma and influence. They must possess values and ethics, and lead by example to affect culture. They need to be visionary and see the future more clearly than most. They need to view the environment as it could and should be, develop the strategy to lead the organization there and anticipate challenges to the vision. And finally, strategic leaders need to have formal and informal training, be extremely knowledgeable about the organization and situation, and have the ability to communicate, negotiate and build consensus. In short, leaders need to be able to "lead, develop and achieve results."[25] Changing an organizational culture doesn't necessarily result in the eroding of the organization's ethics and values. To the contrary, having a solid ethical foundation will help the organization weather the difficulties associated with the change by providing guiding principles for the entire organization. Senior leaders will best serve the organization by living and demonstrating those values and ethics to those they command and by providing the moral compass to their subordinates.

Significant changes to the organizational culture may lead to changes in the Army as a profession. Three culprits serve to widen the gap between the military and the civilian society. They are the military's inability "to adapt its expert knowledge to its new circumstances, officers who believe the values of the military institution were not just different from, but also in several respects better than, those of the society they are protecting, and repeated and well-publicized ethical violations by Army leaders."[26] Changes to the institutional organization as a whole must be evaluated in regard to the soldiers it affects and measures taken in terms of education and training to limit communication problems. The potential effects to the Army profession because of transformation should be anticipated and planned for by Army leaders. Recruiting and training a more diverse force to respond to new and different missions requires more diverse and better prepared leaders. Recruiting more diversity will result in the U.S. Army being more adaptive to new global challenges and more reflective of the society it serves. This will only help in bridging any barriers or gaps that currently exist between the two.

The military still holds fast to many of its norms and values from earlier times. Because of the nature and role of the Army, many of these beliefs and customs are still valid, appropriate and useful. Others should be examined in relation to the values and norms of our civilian society.

The Army is not reflective of the society it represents in relation to regional representation, affluence, education, sexual orientation and gender equality. Today, the South is overrepresented by about eight percent in enlisted accessions each year. In 1996, the South had only 15.4 % of U.S. population, but 31.5 % of military personnel.[27]

The Army recruits more individuals from society's working class and from the poor than from the nation's affluent families. "It is a demographic fact that fewer and fewer of our civilian elites have military service, or that their children are liable to serve in the armed forces."[28] According to a study by the National Priorities Project, more recruits come from families making less than $60,000 annually than those families with higher incomes.[29]

The U.S. Army continues to oppose gays serving in the military and women serving in combat roles even though both issues are fully supported by society. "A December 2003 Gallup poll showed that 79%

of Americans believe that gay men and lesbians should be allowed to serve openly in the military. Over 90% of respondents aged 18-29 agreed that people who are openly gay or lesbian should be allowed to serve in the Armed Forces. More than 80% of those polled think women should either be required to serve in the same combat assignments as men, or should at least have the opportunity to do so."[30]

The U.S. military tends to be traditional, formal and authoritarian. "Unity, self-discipline, sacrifice and placing interests of the group over the individual" have been described as "classic military values."[31] Many members of the Army are also far more conservative in religious and social attitudes and opinions than their civilian counterparts. "It is clear that on certain issues with a religious dimension, such as tolerance of differences in sexual orientation, the views of some military members diverge from those of the population as a whole."[32] Additionally, there are apparent political differences between those serving in the Army and the public. More and more officers, both junior and senior, are identifying themselves as conservative. More military members identify themselves as Republicans more often than do Americans in the aggregate.[33]

In contrast, primary characteristics of the American culture identified by Richard D. Lewis, in *When Cultures Collide*, include individualism, informality, risk oriented, opportunistic, blunt, and competitive.[34] These traits are at odds with the military's need for discipline, order and unity of command. Although most crucial on the battlefield, these attributes need to be standard throughout the Army. If these characteristics are not evident throughout all military ranks, risk exists to individual soldiers, the Army and the Nation. The Army will need to compromise on the individual traits it accepts from incoming recruits while at the same time developing comprehensive training to inculcate the Army's values and norms into the new workforce.

Understanding the Army's own culture and composition, as well as that of our larger society, and being prepared to take actions that closer merge the two will be critical to senior Army leaders who hope to bridge the cultural communication gap.

Recent polling results demonstrate the American public has a high degree of confidence in its military. "In 1975, a Harris Poll reported that only 20% of people ages 18 to 29 said they had a great deal of confidence in those who ran the military. A recent poll by the Harvard Institute of Politics, however, found that 70% of college undergraduates trust the military to do the right thing either all or most of the time."[35] A 2005 Gallup Poll indicates the majority of our society places more trust in its uniformed services than in that of Congress, the clergy, media and the U.S. Supreme Court. "Only three U.S. institutions out of the 15 included in the May 23-26 poll command a high degree of confidence from at least half of Americans: the military, the police, and the church or organized religion. The 74% rating given to the military continues to make it the institution engendering the most confidence of any of those tested – and by a healthy margin."[36]

And yet even with the aggregate polling information, it appears individually that the American view of the military has declined. Don Snyder and Gail Watkins, in their article, *The Future of Army Professionalism: A Need For Renewal and Redefinition,* posit that "recruiting shortfalls, a widening difference in values in perspectives between Americans serving in our Armed Forces, including the Army, and the society they serve, and repeated and well-publicized ethical violations by Army leaders" are issues that indicate a gap between the Army and the public they serve.[37] On one hand, statistics show Americans have faith and confidence in those sworn to protect and defend our nation. On the other hand, this trust does not translate to a significant increase in America's sons and daughters joining the Army, increased military funding or a lack of skepticism and cynicism about the quality and morality of U.S. soldiers in response to scandals and negative media accounts.

Civilian Elite and Political Leadership

The same lack of understanding found between the Army and the general public is also evident in the relationship between the Army and corporate and political leaders. Today, fewer and fewer members of our elected democratic government as well as our civilian elite have any direct knowledge of the Army as an institution. Most members of

Congress have not served in the military nor have they fostered those close, personal relationships with individuals who have. "Only 24% of today's members of Congress have military service, and far fewer have any combat experience. Fewer congressmen have family members serving in the armed forces. At the beginning of the war [Second Persian Gulf War], only one member of the Senate or House had a child serving: six years later the total stands at three."[38] This disturbing trend could have significant impact on the U.S. Army far beyond simply a lack of understanding between the two institutions. Congress provides funding for the Armed Forces. If they do not understand the need for and the requirements of the Army, it is very likely the Army will not receive adequate financial support needed to conduct recruitment and training and for equipping the force. A communication breakdown between policymakers and the Army could lead to poor national security decisions that may ultimately send American service men and women unnecessarily into harm's way or harm international relations.

Our political leaders are not the only significant members of society without a solid understanding of our military. America's civilian elite, many of whom are the country's corporate business leaders, play a vital role in emerging national priorities through economics, status, access and lobbying and yet fewer and fewer individuals from our society's middle and upper classes have any direct knowledge of the military. Those civilian leaders who are unaware or uninformed of the role, mission and needs of the Army may at best be apathetic toward the military. Worse, they may intentionally oppose the Army. Due to their status within the communities and government, this could lead to lack of funding or the implementation of poor policies. Peter A. Gudmundsson opines in an article published in the *Christian Science Monitor* that veterans with their better understanding of the military, thus better represent society. "A society with veterans represented at all levels of the community is better equipped to interpret accounts of inadvertent civilian casualties, interrogation interpreted as torture, or prisoner abuse. With the abdication of the upper classes from military service, most elites in the media, private sector and government service don't have the intimate human context for the realities of war."[39]

Strategic Communication Initiatives

The U.S. Army needs to enhance its strategic communication efforts and reexamine its relationship with the media in an effort to improve communications with the U.S. public. In too many instances the Army has considered the media as something it had to deal with in a negative environment instead of viewing the media as an opportunity to multiply and maximize its efforts to communicate to the American public. Scandals and bad news stories are going to continue to occur within the Army, and with enhanced technology and 24-hour news cycles the Army can be certain there will be reporters on the scene. But instead of focusing the majority of its efforts responding to negative news stories, the Army should focus its efforts on developing relationships with reporters, editors, on-air personalities and bloggers, and in developing strategic and operational communication and information campaigns as an integral part of our military and political planning. To better connect with American society, the Army needs to engage the media, not just deal with it.

Transformation is necessary if the Army is to bridge the civil-military gap existing between the Army culture and society and continue to recruit and retain an educated and professional all-volunteer force. Developing strategic communication initiatives and employing them throughout all levels of the Army will be required. Additionally, options deemed off the table for consideration in the past, to include allowing women in combat, homosexuals to serve openly, and reinstating the draft, need to be reevaluated and examined for merit and validity from the perspective of our changing cultural environment as well as from the need to maintain and improve the institutional Army.

Just like providing all the resources necessary for the U.S. Infantry to fight and win our Nation's wars during conflict, the Army must make a commitment to develop a program, raise a staff, and provide training and equipment for a strategic communication office if it is to win the cultural communication war in between the military and society.

> *New institutions are needed for the 21st century, new organizations with a 21st century mind-set. For example, public relations was invented in the United States, yet we are miserable at communicating to the rest of the world what we are about*

> *as a society and a culture, about freedom and democracy, about our policies and our goals. It is just plain embarrassing that al-Qaeda is better at communicating its message on the internet than America. As one foreign diplomat asked a couple of years ago, 'How has one man in a cave managed to out-communicate the world's greatest communication society?' Speed, agility, and cultural relevance are not terms that come readily to mind when discussing U.S. strategic communications.*[40]

Establishing a Strategic Communication Office (SCO) at the Department of the Army would be an ideal starting point. The goal of this office would be to develop strategic messages, identify audiences, and measure message effectiveness. The SCO would rely on elements of the rest of the Army to include Public Affairs, Legislative Liaison, Speechwriting Staff, and Recruiting Command's Advertising and Marketing team to meet its objectives, but more importantly to assist with message deployment. "The most difficult part of strategic communication is finding a means to get the message to the intended audiences. Not only is that difficult in itself, but the sender must cut through all the static, clutter, and competing messages flooding the scene. This solution is straightforward even if complicated – use every channel possible and as many as possible."[41]

The key to the success of the SCO is to have enough power or influence to ensure the commitment and participation of the entire Army. Army senior leaders must be personally involved to ensure the Army's priorities are properly and fully communicated to internal and external audiences. Messages need to be developed based on the organization's core values. They must be pertinent, concise, resonate with audiences and be meaningful and appropriate for use by all Army elements to include National Guard, Reserve and the Civilian Corps. And effective messages will need to be developed, staffed and deployed decisively and quickly. As message development involves more than simply words, it is imperative that the Army focus on actions as well. The SCO will need to coordinate closely and provide strategic guidance and themes for all elements of Army marketing programs, such as the U.S. Army Bands, The Golden Knights, the 82nd Airborne Division Chorus, The Old Guard, and The Army Marksmanship Team. Information should be coordinated and synchronized to achieve maximum effect, but the execution should continue to be decentralized.

Since recruiting quality individuals in sufficient quantity to serve in the U.S. Army is and will remain a strategic challenge, it is imperative that Army leadership be personally involved in planning for the future composition of the Army. Leadership engagement will provide the strategic vision necessary for the organization to successfully meet and exceed its recruiting challenges. Changes to Army recruiting resulting in impacts on the Army culture, climate, ethics and profession should be anticipated and planned for to develop the most effective path ahead.

Currently, the U.S. Army Recruiting initiatives, programs and incentives targeted at the 17-24 year-old market have allowed the Army to meet its annual recruiting goals. The advertising, information and marketing campaigns conducted by the Army's advertising agency and Accession Command are well researched, developed and executed for this target audience. Inducements such as the Army College Fund have been and continue to be the only option for many individuals to obtain a college degree. As such, the program has been a highly successful initiative. Flexible options that allow today's youth to use this program should continue to be examined and extended. Recent enlistment bonuses and enticement programs such as money for homebuyers are creative and beneficial initiatives that are of interest to recent high school graduates as well as older, eligible potential recruits. The Army should also consider expanding Junior Reserve Officer Training Corps (JROTC) programs in high schools and ROTC in colleges to further encourage youth of the benefits of the Army.

The Army needs to spend more time and resources influencing two additional markets in order to maximize overall recruiting efforts. The first is centers of influence or the parents, coaches and educators market. The goal is not necessarily to have this segment actively promote the Army as a career to the target market, but instead to provide them with enough information, knowledge and comfort level of the organization so that they will not discourage teens who are considering enlistment from joining. The Army should continue its advertising campaign directed at this group, but additionally, should expand its outreach efforts. One-on-one contact is essential and Recruiting Command and other Army leaders should engage local community organizations as much as possible. Providing guest speakers for civic group events, and actively participating in community functions and activities will assist in this effort. Programs to reach educators, guidance counselors and high school coaches throughout the United States should continue to expand. In underrepresented areas that have little contact with the active duty Army, this group should be taken to Army installations for tours, briefings and to see basic training firsthand.

The second population the Army needs to concentrate its efforts on is junior high and middle school aged children. This should not be done from a recruiting perspective but more as a way to assist with education, mentoring and physical fitness programs. The Army should work with school systems and administrators to develop a collaborative campaign to further assist students. Fewer and fewer schools are teaching military history. Adolescents are experimenting with alcohol, tobacco and drugs at younger ages, many before they are 13 years old. A Center for Disease Control (CDC) study asserts that every day there are approximately 4,000 children, aged 12-17 years old who smoke their first cigarette. The CDC also warns of the number of children whose health is at risk because of weight and inactivity issues.[42] If the Army wants to better connect with the society it protects, then it needs to be directly involved in community solutions. It won't be an easy or quick fix, but should be incorporated to improve communication with the American public. "Winning hearts, minds, trust and credibility, in the end, requires a local approach."[43]

Ultimately, if the Army is serious about creating an organization more in tune with those it represents while continuing to meet its recruiting challenges, it needs to work to change laws and regulations in order to expand its recruiting pool to all qualified applicants for all positions regardless of gender or sexual orientation.

Allowing homosexuals to serve openly and allowing female soldiers who are physically qualified to serve in combat roles would leverage diversity. "Leveraging of diversity, or capitalizing on diversity, means turning diversity into an advantage by using it to enhance performance and social legitimacy."[44] If the Army is serious about recruiting youth from Generation Y, it needs to prove it is an organization reflective of society and open to those with different beliefs, ideas and opinions. "The attitudes of younger Americans in general and high school students in particular are especially relevant to the future military, because today's high school students represent the Army's major recruiting pool and its source of future officers, and represent as well the nation's future civilian leaders, policy-makers, and voters."[45]

Additionally, it is unlikely in the long run for these types of changes to degrade military effectiveness or negatively affect cohesion or ultimately performance. "The evidence for a relationship between cohesion and group performance shows that it is task cohesion, not social cohesion that is related to success."[46]

This option is bound to be a tough sell for many both inside and outside of the military. However, integrating African-Americans and women into the Armed Forces proved to be a controversial initiative in its infancy as well. Leaders charged with the organizational changes faced cultural and climate issues as those reforms challenged long-held Army beliefs and traditions. Because of leadership vision, strategy and willingness to stand behind the changes and lead by example, the transformations occurred and made the Army a better organization that is more reflective of the society it serves. These developments profoundly changed the culture and the climate of the organization and prove significant changes to an institution's culture can be accomplished. "At a time of stark tensions and continuing separation between the races, not only is the Army a thoroughly integrated institution, its members seem at peace with the idea."[47]

Establishing improved communication with our political leaders will take a robust, well trained legislative liaison office that not only responds to Congressional questions and requests, but improves outreach programs to legislators that explain, inform and demonstrate the Army's roles, missions and capabilities. This should be done in coordination with the messages and guidance from the proposed SCO, so that the Army speaks with one voice. This could be accomplished through continued efforts to incorporate one-on-one meetings, briefings, office visits, testimony, information papers and reports, and through a Distinguished Visitor Program to Army installations where political leadership see Army training and meet soldiers. More soldiers and Department of the Army civilians should be afforded the opportunity to participate in the Army's Congressional Fellows program where they are afforded the opportunity to work in a Congressional staff office to learn more about the legislative process. This increases knowledge and understanding for both the soldier and DA civilian as well as for Congressional staffers and members. It also serves to develop relationships and improve communication processes between the two organizations. In addition to sending Army assets to work on the Hill, a program to embed Congressional staffers into Army staff offices should also be implemented in order to give these individuals a better understanding and education of the military. Although not a quick fix, a comprehensive plan to better inform political leaders about the Army is essential in bridging the cultural communication gap between the two institutions.

The Army would also be well served to conduct an educational outreach campaign targeted at U.S. Chief Executive Officers and state and local political leadership. Armed with strategic themes and messages, the Civilian Aides to the Secretary of the Army (CASAs) and the Army's retired general officers could be instrumental in serving as liaisons to various groups of influencers throughout the country.

Army leaders throughout the organization need to do a better job of encouraging two-way communication and open dialogue within the Army. Senior leaders should strive for a culture of innovation within their organizations. "A culture of innovation is typified by an environment within which every single person in the organization is invested in the organization's success and feels a responsibility to implement new and better ways to achieve organizational objectives."[48] Although junior leaders and young enlistees need to be cognizant of the Army's culture, chain of command and need for good discipline and order, senior leaders need to be more aware and responsive to Generation Y's culture and preferred communication styles. Implementing or continuing to teach diversity and communication training throughout the Army will assist in garnering improved communication.

The Army needs to find ways to reduce bureaucracy, which should help improve communication when it comes to implementing change. The communication issues related to transforming the entire institution's roles and missions since the end of the Cold War have been hindered because of the lack of creative thinking and the reluctance of some in the process to change the way we do business. The Army must demonstrate learning organization behavior in order to grow and thrive. "Learning organizations are organizations where people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective aspiration is set free, and where people are continually learning to see the whole together."[49]

Conclusion

A divide between the U.S. Army and the American public it serves currently exists. Concerns that the gap continues to widen are real and tangible. As the world evolves, more and more U.S. citizens have less direct contact or knowledge about soldiers, the Army or the military in general. Those who comprise the Army are more educated, more politicized and find themselves more isolated from many of those segments of society they have sworn an oath to protect and defend. Many in the military view themselves not just different from society, but better.

In *The Art of War,* Sun Tzu contends that by knowing your enemy and yourself, you will avoid peril.[50] The U.S. Army's enemy is not the American public. It is the inability to understand and engage a changing culture and to develop a strategic roadmap to effectively communicate to target audiences about the role, mission and need for an Army. To be successful, the Army will need to improve efforts to be a learning and changing organization. To thrive, and not simply to survive, will require the Army be flexible enough to move away from many traditional ways of doing business, take more risks and find innovative means to market and explain itself. This transformation must begin with Army leadership. A primary and important role of strategic Army leaders is taking responsibility for bridging the cultural communication gap between the American public and the Army. This will be an ongoing effort requiring constant attention and due patience and the Army will need to make strategic communication initiatives a priority in order to really affect the environment. Strengthening relationships between the military and the public, educating and informing society of the role and need for the U.S. Army, and recruiting soldiers who are reflective of the society we live in will be essential if the Army is to continue to play a vital role in the defense of this nation.

Section Two

Information Effects in the Physical Domain

Prudens
Futuri

Introduction

Colonel Jeffrey L. Caton
Director, Research, Development, and Acquisition Management
and Defense Transformation Chair
Department of Command, Leadership, and Management
U.S. Army War College

Network Centric Warfare (NCW) encompasses activities within the information, cognitive, social, and physical domains. The Department of Defense (DoD) recently validated its definition of cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] Clearly, this includes reference to physical elements and systems. Thus, cyberspace operations depend on physical infrastructure and such operations can affect the physical domain.[2] This section focuses on information effects in the physical domain, and it features U.S. Army War College Academic Year 2008 papers that examine the implications of NCW and cyber warfare for future national security operations. The reader will notice three common themes advocated within the papers: achieving interoperability; approaching NCW in a holistic view; and considering organizational and cultural challenges when implementing change.

Lieutenant Colonel Duane T. Carney, U.S. Army, earned the Red River Valley Fighter Pilot's Association Writing Award for his strategy research paper, "Unmanned Aircraft Systems Role in Network Centric Warfare." He provides a brief background of the increasing relevance to theater commanders of unmanned aircraft systems (UAS) as part of NCW. Next, he analyzes the various roles of UAS to facilitate information dissemination and to relay communications as well as the ability of UAS to operate in a constrained frequency spectrum environment. His discussion includes details on the evolution of UAS applications within the Army's current modular brigade forces as well as those planned for the Future Combat System program. Noting that "fully integrating UAS within these operational theaters continues to challenge military leaders," Colonel Carney offers three specific recommendations to facilitate continuing transformation efforts toward the DoD vision of NCW.

Lieutenant Colonel Michael M. Sweeney, U.S. Marine Corps, received the U.S. Army War College Foundation Award for Outstanding Strategy Research for his paper, "Blue Force Tracking: Building a Joint Capability." As proven force enablers, Blue Force Tracking (BFT) capabilities help provide critical situational awareness at all echelons within today's complex battlespace. Colonel Sweeney describes elements of typical BFT systems as well as how they address the age-old military questions: "Where am I? Where are my forces and other friendly forces? Where is the enemy and what is the best route to attack him?" He presents the challenges of developing a truly joint BFT capability "required for tomorrow's fight that resolves the peer-to-peer data sharing issues while reducing the burden on satellite assets." He highlights the role of accelerated development processes, such as Advanced Concept Technology Demonstrations and Urgent Need Statements, in the evolution of BFT systems and argues that "collectively, these factors have exacerbated the interoperability challenges faced today." Almost one-third of Colonel Sweeney's paper focuses on detailed recommendations to achieve successfully the anticipated exponential growth of BFT-related devices planned through 2015.

Lieutenant Colonel David P. Acevedo, U.S. Army, in his paper "Providing an Enterprise Service Architecture to the Net-Centric Warfighter," promulgates a vision for future joint forces with "full spectrum dominance through the use of networks and access to enterprise data services that provide true interoperability, seamless integration and available on demand collaboration." He argues that achieving this capability requires a joint strategy which uses Resource Forest (RF) architecture "that strikes the right balance between control, security, autonomy and flexibility." To set the stage for discussion, he provides a short primer of Active Directory and its NCW applications. He specifically addresses challenges of having rapid connectivity and continuity of operations for modular units as they deploy, including cogent observations from Operation Iraqi Freedom. Colonel Acevedo outlines the advantages and disadvantages of RF architecture applications and closes with overarching recommendations for implementing this architecture as well as enhancing a culture of jointness.

Captain Paul M. Shaw, U.S. Navy, examines potential NCW-related organizational hurdles in his paper, "Achieving DoD's Net Centric Vision of Information Sharing While Overcoming Cultural Biases to Control Information." He presents the challenges of shifting from an inflexible "need to know" information environment to a more desirable "need to share" collaborative culture. He uses the classic "ends, ways, and means" strategy model to frame his discussion which includes a concise survey of current DoD information sharing policy as well as the associated cultural biases. Captain Shaw identifies key elements of potential technical solutions and proposes three options to enhance future NCW partnerships. He concludes that achieving such an information sharing vision requires an understanding of the "balance of the human, policy, process, and technology."

What is the relevance of the issues examined in these papers? First, they support key guidance provided in the 2008 National Defense Strategy to "continue to develop innovative capabilities, concepts, and organizations" – such as those described in these papers. This, in turn, helps fulfill the need to provide "not only have a full spectrum of capabilities at our disposal, but also employ and tailor any or all of them to a complex environment."[3] Second, they further define policy for NCW systems that "improve economic efficiency by eliminating stove-pipe systems, parochial interests, redundant and non-interoperable systems, and by optimizing capital planning investments for present and future information technology systems."[4] Finally, they help to provide a framework for critical thinking to participate effectively in the 2010 Quadrennial Defense Review as well as to support current CJCS Guidance to "identify instruction, policy, and technology approaches that remove impediments to information sharing with each other, our partners and leverage our combined knowledge strengths."[5]

Unmanned Aircraft Systems Role in Network Centric Warfare

Lieutenant Colonel Duane T. Carney
United States Army

Military history includes technological advancements that have significantly altered the conduct of warfare. Some examples include machine guns and enhanced field artillery in World War I, vastly improved airplanes and tanks during World War II, and helicopters used for air mobility in the Vietnam War. Currently, the United States has been at war for 6 years – what is the icon of today's battlefield? Perhaps Unmanned Aircraft Systems (UAS) should join this list. While this paper does not support or refute this proposition, it does argue that the proliferation of UAS has significantly affected combat operations. Current operational theaters serve as proving grounds for both mainstream and experimental UAS, and many of these systems have successfully supported commanders' situational awareness requirements. Wartime commanders are increasing their requests for capabilities that UAS provide. The Department of Defense's (DoD) actions to fulfill these requirements attest to their growing relevance. Like many of the technical capabilities being fielded as part of DoD transformation, UAS require communications networking resources to operate and to realize their maximum potential. However, fully integrating UAS within operational theaters continues to challenge military leaders. DoD cannot fully implement its vision of Network Centric Warfare (NCW) without fully integrating UAS within the theater communications network.

This paper examines the role of UAS in NCW. First, it provides a brief background on NCW and UAS to establish their distinct relevance. Next, it explores three key considerations necessary to fully integrate these two elements: the role of UAS in facilitating information dissemination, the role of UAS as an aerial communications relay, and the ability of UAS to operate within a constrained frequency spectrum environment. It then concludes with recommendations for establishing UAS as a valuable theater asset within the NCW environment.

Network Centric Warfare: A Matter of Department of Defense Transformation

To meet the Nation's global wartime imperatives, the President's 2006 National Security Strategy highlights the need to "transform America's national security institutions."[1] Accordingly, the DoD is transforming to provide joint-force capabilities designed to meet an increasing array of challenges. This transformation includes the integration of advanced information and communication technologies to enable rapid information sharing across the battlespace. The operational benefits derived through this infusion of networked capabilities are commonly termed "network-centric capability" or "net-centricity." The DoD Forces Transformation and Resources office maintains that enabling NCW is at the heart of U.S. military transformational efforts.[2] But what precisely is NCW and why is this concept relevant to UAS?

To answer this question, first consider these basic NCW tenets:

- A robustly networked force improves information sharing
- Information sharing and collaboration enhance the quality of information and shared awareness
- Shared situational awareness enables self-synchronization
- These, in turn, dramatically increase mission effectiveness[3]

Not focused exclusively on technology, NCW seeks to empower military commanders by providing them with enhanced situational awareness and information superiority. The military services currently rely on their individual funding to field networked communications and electronic systems that achieve this operational advantage and to meet warfighters' increasing information demands. Collectively, these efforts account for about $65 billion of DoD's 2007 budget.[4]

Recent operations have exhibited a dramatic growth in intelligence, surveillance, and reconnaissance (ISR) information requirements ranging from the individual tactical soldier all the way to the combatant commander's joint operations center. In response to these demands, military services have fielded UAS rapidly, thus providing access to critical information and gaining popularity through their demonstrated successes. For example, the 2006 Quadrennial Defense Review report describes a vignette where a deployed ground force in battle coordinates with UAS pilots in Nevada, who then direct UAS to support combat operations – all facilitated by the power of network connectivity.[5] While this example is impressive, UAS of varying sizes, capabilities, and missions are arriving in the battlespace in increasing numbers.[6] NCW, a concept central to DoD transformation, is executed through the networking (or interconnectivity) of critical battlespace elements to enhance combat effectiveness. However, does NCW fully include a large-scale integration of UAS? Moreover, what is the relationship between UAS and the "network," and how is this relevant? To address this, the author argues that UAS are a vital capability with increasing strategic and operational relevance, and that there are operational benefits to fully integrating UAS into the theater communications network.

Unmanned Aircraft Systems: Doing the Dull, Dirty and Dangerous[7]

While earlier deployments exist, successful UAS operations in Iraq and Afghanistan have brought this capability into global prominence. UAS provide tactical and strategic ISR capabilities into the theater by providing full-motion video (FMV), imagery, and sensor information in real time to the commanders, significantly increasing their situational awareness. Traditionally used only as an ISR asset, UAS now provide additional battlespace functions such as strike capabilities, air interdiction, and aerial communications relay. There is great potential for UAS capabilities, a fact recognized by both the combatant commands and the military service departments. Specifically, UAS could fulfill 17 of the DoD's 99 prioritized capability gaps (2 of them in the top 10), an inclusive list using input from all services, the fiscal year (FY) 2008-2013 Combatant Commanders Integrated Priority List, global counter terrorism planning requirements, and lessons learned analysis.[8] This demand has not gone unnoticed. According to the Government Accountability Office (GAO), the DoD's FY2008 budget request includes 2.23 billion dollars for UAS – this represents a 600 percent increase from 2001.[9] The significant increase in the number of UAS, from 50 systems in 2000 to a current level of approximately 3,900, further suggests growing operational relevance. Most of the available UAS in the DoD inventory now serve within Iraq or Afghanistan.[10]

The DoD categorizes UAS into three classes. Man-portable UAS are hand-held devices designed to support small ground elements. Tactical UAS have greater capability (longer loiter times, more coverage distance) and offer increased video and sensor services with more robust product distribution.[11] Theater level UAS support theater-wide requirements by providing even more robust capabilities; they require significant network resources.[12]

A typical UAS consists of four basic components. First is the aircraft (fixed or rotary wing) and its associated payload. The payload varies according to the UAS size and mission, and may include weapons, sensors, FMV apparatus, and communications equipment. Second is the Ground Control Station (GCS) which serves as the control hub directing the UAS operation. Larger, theater-level UAS (such as the U.S. Air Force Predator) require significant GCS equipment and facilities, portions of which may be located outside of the operational theater. Third is the associated communications architecture connecting the UAS to the GCS; it ensures control of the aircraft and receives collected products. This architecture ranges from a simple line-of-sight structure supporting man-portable or tactical UAS to more complex satellite-based architecture supporting theater-level UAS. The fourth component is the associated viewing apparatus, such as the Remote Video Terminal (RVT) used to receive FMV directly from the aircraft.[13] To operate effectively, all UAS classes require theater communications resources such as available frequency spectrum (referred to as bandwidth) and networking architecture.

The Defense Department is making considerable strategic investments in UAS and is promoting NCW as part of military transformation. But are these two pursuits mutually supportable, or divergent? The 2006 QDR clearly links the two objectives, stating that the DoD remains "invested in new equipment, technology, and platforms for the forces, including…unmanned vehicles…all linked by Net-Centric Warfare Systems."[14] However, current operational demands to field UAS rapidly have created significant theater network issues. In fact, the DoD is currently unable to realize the full operational potential of UAS effectiveness. GAO testimony cites continued challenges in network interoperability and spectrum availability as two main impediments to current employment of joint UAS.[15]

The DoD cannot successfully implement NCW without fully integrating UAS within the theater communications network – but what does this task entail? This paper examines three requirements for UAS in robust, fully functional NCW: information dissemination, aerial communications relay, and operation within a constrained frequency spectrum environment.

Information Dissemination: Establishing Situational Awareness

As described by its tenets, NCW strives for an operational advantage by providing relevant information to the right place, at the right time, and in the right format. Increasing UAS numbers, along with their expanding ISR missions, are prime candidates to function fully within this environment. To achieve this goal, UAS must provide widespread and networked access to the information they provide, and this presents significant implications for the theater communications architecture. When discussing effective UAS integration, General William T. Hobbins, Commander, U.S. Air Force Europe, states that:

> *It's got to go to the core of operations. The information from (UASs) could, and I contend, should populate the global information grid [GIG[16]], to the maximum extent possible. Systems of systems can provide the appropriate information at the right time to those who need it. This would correspond to improve situational awareness at all levels of warfare. … It's about decision superiority.*[17]

Creating an "information stovepipe" where UAS data is transmitted to a single location provides value only to a limited audience. The situational awareness information that UAS provide greatly add to the "common operational picture" of the battlespace. But should everyone have access to this information? Should all UAS information populate the theater information grid? Answering these questions serves two purposes central to a discussion on information dissemination. First, it forces a disciplined approach to addressing information exchange requirements (who needs the information and therefore, where does the information need to go). Second, it highlights interoperability requirements between the UAS components and the theater communications architecture (how effectively the information gets to their destinations).

Each military service seeks to codify information demand and exchange requirements, in part, to properly train and equip their organizations. This is an imperfect science, since requirements vary at the tactical, operational, and strategic levels. Two brief data points shape this discussion. First, DoD has stated that it is technologically impracticable to provide full access to products derived from man-portable UAS.[18] Accordingly, this analysis will focus on operational and strategic level UAS unless otherwise noted. Secondly, leaders should beware of the "transfixing" effect that UAS video can have on personnel within command and control facilities. Real-time ISR video feeds can become the center of attention – or distraction – of those not directly involved in that mission. In fact, a recently published multi-service UAS manual warns that "access to real-time UAS video requires discipline and dedication to viewing the imagery only when necessary and by those who have a need."[19]

While the services may not fully define all information requirements, operational and strategic UAS must enable common access to their information products to be relevant assets within NCW. Such access requires interoperability with the network transport and data systems within the theater communications architecture. However, the GAO has cited lack of interoperability among the various UAS components and current communications systems as a major impediment to joint operations.[20] To meet military demands, DoD rapidly designed, fielded, and enhanced UAS. Traditional acquisition processes that govern DoD programs of record do not always facilitate the rapid infusion of the technological advancements sought by deployed military units.[21] Unfortunately, time saved in quickly fielding service-specific UAS has also affected their ability to operate jointly. Each service, as well as U.S. Special Operations Command, is developing UAS to support all military echelons from the small unit level to the Joint Force Commander. "In fact, by 2010, DoD plans on having at least 14 different UAS in the force structure to support a variety of missions."[22] Additional experimental UAS variants will add to this number and contribute to the interoperability challenge. Lack of interoperability creates further engineering challenges for theater network planners — at times resulting in less than ideal architectural solutions. In worse cases, lack of interoperability breaks the information flow and prevents information-sharing altogether.

To establish uniform standards and provide executive-level oversight, DoD established the UAS Task Force with a mission to "lead a Department-wide effort to coordinate critical UAS issues, and to develop a way ahead for UAS that will enhance operations, enable interdependencies, and streamline acquisition."[23] One significant product developed by the UAS task Force is the recently published *Unmanned Systems Roadmap 2007-2032,* which serves as Office of the Secretary of Defense-level guidance regarding future development, funding, and prioritization efforts across DoD.[24] Considering past difficulties with integrating UAS in a joint environment, standardization and interoperability are main goals for DoD. Indeed, each service understands the operational and logistical benefits derived from adhering to a coordinated DoD UAS acquisition strategy. For example, Brigadier General Stephen Mundt, Director of Army Aviation, reported in his congressional testimony that a principal goal of Army UAS strategy is commonality. Contributing to this commonality is the Army's "One System Ground Control Station (GCS)." This equipment, also pursued by the U.S. Marine Corps promotes interoperability among Army UAS and will allow a greater degree of operational flexibility while simplifying training and logistics requirements. This GCS employs the Tactical Common Data Link (TCDL), which provides the data link from the aircraft and promises significant interoperability improvements.[25] Knowing that his Congressional audience remains deeply concerned over costly and divergent acquisitions, Brigadier General Mundt emphasized that:

> *The One System will be…TCDL compliant, which will provide us a more reliable datalink and more efficient use of the frequency spectrum. The One System will also be NATO Standardization Agreement 4586 compliant which will provide us interoperability across joint and coalition unmanned systems.*

> *The One System concept has already peaked interest with our NATO partners. They understand the power of having a single set of ground equipment that can interoperate with an entire fleet of joint and coalition unmanned aircraft.*[26]

The DoD recognizes the value of employing TCDL across all services as one of its primary objectives to achieve interoperability.[27] To improve information dissemination, the U.S. Army is fielding the One System Remote Video (OSRVT) terminal to its deployed forces. OSRVT is a lightweight (portable or platform-mounted) system capable of receiving broadcast images from several UAS simultaneously.[28] While these are steps in the right direction, they addresses only a portion of the problem. Many UAS still pass their critical video, sensor, and control information to a single Ground Control Station in a closed circuit fashion, thereby isolating the UAS from the theater network and other battlespace elements.[29] Often, users must rely on separate networking solutions to receive different UAS products.

One example of such a separate network is the Global Broadcast Service (GBS) program, which offers high-speed, one-way flow of information (video and data) to deployed and garrisoned users. Additional theater communications resources must transmit the UAS video from the local source to a GBS data injection point, perhaps located outside of the country of origin. In turn, GBS satellites transmit video back to users located in the theater.[30] Certainly, such videos travel a long way to get disseminated throughout the theater battlespace. This example is not intended to denigrate the GBS program. In fact, this program currently provides an invaluable product to the warfighter. The existing theater network simply cannot disseminate the large amount of UAS video required throughout the region. NCW requires consolidation of networking solutions to enable rapid information exchange, to enable users to query relevant information sources, and to promote positional awareness of key battlespace elements.[31] For UAS to be a viable part of the NCW environment, they must be able to "plug" directly into the theater network. Common GCS using TCDL is a start, but DoD must provide a communications network interface to complete the architecture.

One such DoD program may fulfill this requirement – the Warfighter Information Network-Tactical (WIN-T), which offers promise for enabling effective UAS information dissemination. WIN-T is a multi-billion dollar Army program that has the documented requirement to provide a single integrated communications network that promotes joint interoperability and enables linkage of battlespace sensors to the GIG. WIN-T is designed to eliminate the need for current non-interoperable networking solutions. It also provides a much needed communications-on-the-move capability for all echelons. Inherent within the WIN-T concept is the full network integration of UAS to maximize network capacity and efficiency, and to improve information dissemination.[32]

Information requirements must include interoperability that enables military and commercial systems to communicate with each other efficiently as well as provide broad access to their products. UAS information dissemination provides an important contribution toward achieving battlefield situational awareness. All UAS components must take into account the current and future capabilities of the communications network, and vice versa. Both UAS and the network are co-equals in NCW. Clearly, UAS need the network to disseminate its products but, how can UAS assist the network to provide communications connectivity throughout the battlespace?

Building the Aerial Communications Layer

As stated previously, NCW requires the networking of personnel and battlespace command systems to enhance overall combat effectiveness. Building this omnipresent network connectivity continues to challenge the theater commander. Traditionally viewed as only an ISR asset, one emerging role of UAS may offer a substantial contribution to this situation. To realize the benefits envisioned by advocates of NCW, DoD must broaden the ability of UAS to provide communications connectivity throughout the battlespace, in effect serving as a "network multiplier." Functioning as an aerial communications relay node, UAS provides the ability to extend the network to more units operating at greater distances as well as within urban or adverse environments. Given the almost insatiable appetite for the network applications, theater planners continue to increase the use of UAS as aerial relay nodes. In fact, of the 16 different mission areas associated with theater UAS, Combatant Commands ranked "communications/data relay" as fourth.[33] The following section argues that UAS serve a growing and significant role in enabling NCW through their ability to extend the network. This analysis focuses on DoD's approaches to building the aerial communications layer and addresses associated opportunities and challenges.

What is meant by an 'aerial communications layer' and why is it required? Answering these fundamental questions requires a look at the conduct of current military operations and requires a brief scan of future joint operational concepts. Today, U.S. forces are spread out over great distances, operating in urban as well as mountainous terrain, and often arrayed in non-contiguous fashion. To support these units, the network requires an architecture consisting of three layers, or tiers—terrestrial, space, and aerial. Traditional line-of-sight communications (the terrestrial communications layer) do not operate consistently within this environment due to physical obstructions. Satellite resources (the space communications layer) are not readily available or responsive enough to support both planned and ad hoc requirements. However, an interconnected third tier within the network, the aerial communications layer, ensures not only adequate coverage but also adds sufficient redundancy to mitigate risks from overreliance on a given group of transmission systems.[34]

What about future joint operations? Strategic military publications offer clear insights to future joint warfighting capability requirements. The 2005 National Defense Strategy cites the ability to conduct network-centric operations as one of DoD's "key operational capabilities" required to ensure effectiveness of a highly distributed force.[35] In describing future capabilities, the Capstone Concept for Joint Operations declares that "the joint force will capitalize on being networked…and will exploit network connectivity among dispersed joint force elements to improve information sharing, collaboration, coordinated maneuver, and integrated situational awareness."[36] The supporting Joint Functional Concepts (Command and Control, Force Application, Protection, Focused Logistics, Battlespace Awareness, and

Net-Centric Environment) all tout their respective domain requirement for a ubiquitous network. While DoD continues to program and field improvements for terrestrial and space communications capabilities, limitations persist and requirements keep accumulating.[37]

The essential question is: Can the network meet these future expectations? In the extreme case, no network equates to no NCW. Given the existing impediments to DoD transformation and future joint operations, leveraging UAS to increase network robustness and to provide access to otherwise disadvantaged users is a pursuit worthy of serious consideration. In fact, a DoD-sponsored study concluded that total satellite demands will exceed requirements without the establishment of an aerial communications network.[38] The U.S. Army Signal Center supports this conclusion by asserting that future network capacity will meet only half of military requirements; the Signal Center therefore strongly advocates development of an aerial communications layer to redress this shortfall.[39]

Fortunately, DoD has several efforts underway to develop such capability. The military services are on a path to build an aerial layer communications capability using either manned or unmanned platforms. The Air Force's Objective Gateway, a funded acquisition program, is designed to field an airborne network relay and communications gateway to link up various air and ground elements. As a key part of this program, the Battlefield Airborne Communications Node (BACN) provides an airborne communications relay package and data information server. Although the Air Force is currently testing BACN on a manned aircraft, program technicians anticipate integrating this system within a UAS.[40] The Marine Corps provided their Marine Airborne Re-Transmission System (MARTS) in response to urgent requirements from their deployed units. This experimental program, developed by the Defense Advanced Research Project Agency, fields a tethered, unmanned airship that relays radio communications within an area with a radius in excess of 68 nautical miles.[41] The Navy is pursuing similar aerial communications relay capabilities to support their fleet.

To meet current demands and future requirements, the Army is making a considerable effort to provide a UAS tactical aerial communications relay. Although ISR remains a primary mission, the Army's Shadow UAS also provides radio communications relay to brigade-sized elements.[42] Further, the Hunter (and starting in 2009, the Sky Warrior) provides a division-level UAS capable of supporting communications relay missions. To address the reality of competing UAS priorities, the Warrior is designed to execute multiple missions, such as simultaneous ISR support and communications relay.[43] While these examples suggest a growing Army interest in using UAS as an aerial communication relay, what is more indicative of Army commitment is the envisioned role of that capability within high-level acquisition programs: Future Combat Systems (FCS), WIN-T, and the Joint Tactical Radio System (JTRS).

The 2007 Army Modernization Plan asserts that FCS is the "cornerstone of the materiel modernization of the Army" and is central to the Army's relevance in the 21st century. This multi-billion dollar program fields an interoperable mix of 14 manned and unmanned systems. Through the power of network technology, FCS provides situational awareness to all platforms, right down to the individual soldier. Originally designed to field four different UAS, FCS will now include a Class I and Class IV UAS.[44] Among its mission capabilities, the Class IV UAS, currently designated the Fire Scout, provides aerial communications relay coverage. According to the Army's concept, to achieve their maximum capability an FCS brigade

> *...leverages all available resources to provide a robust, survivable, scalable and reliable heterogeneous communications network that seamlessly integrates ground, near ground, airborne and space-borne assets for constant connectivity and layered redundancy.*[45]

The Army's WIN-T program and the DoD's JTRS program will provide this network transport layer to connect both FCS brigades and today's modular brigade forces. To address future network demands, both programs also provide aerial communications relay packages for UAS. In general, DoD has just begun to develop aerial communications relay capabilities. The services continue to pursue this capability for a simple but telling reason – they require more network access than they currently possess.

Using UAS for this mission presents both opportunities and challenges for DoD as well as for advocates of NCW. Potential benefits include addition of means to extend the network to those who would otherwise remain isolated. Aerial communications relays could serve as an alternative to terrestrial systems that functionally rely on line-of-sight and protected territory to function – both being problematic in counterinsurgency operations in urban and complex terrain. It also provides an alternative to costly and limited satellite resources – which often cannot respond quickly to short-notice demands.

With these potential benefits, however, come significant challenges. Separate service-led pursuits increase the risk of exacerbating the interoperability problems first realized in integrating UAS within the joint operational environment to execute ISR missions. Without established program standards and technical protocols for developing an aerial layer tier, DoD may not provide a capability that interoperates with existing and future data and transport architectures. To efficiently integrate an aerial tier within the theater network, units need appropriate concepts and doctrine that provide network management and planning guidance. UAS aerial communications relay missions must expand the network in a predictive and responsive manner which may conflict with other UAS mission requirements (e.g. ISR) deemed a higher priority by unit commanders. Finally, in order for UAS to further enable NCW as an aerial communications relay, DoD must address a problem that continues to plague the operational success of current UAS ISR missions as well as many other systems – lack of available operating spectrum.

Spectrum Availability – Making the Magic Work

While not all military leaders care to understand the technology that enables electronic systems found throughout today's military environment, there is one fact that most experienced leaders now understand – they need bandwidth to make the "magic" work. More precisely, the availability of frequencies within the electromagnetic spectrum allows many of these systems to operate. However, the lack of spectrum availability continues to impede current military operations. According to a 2007 GAO report, UAS suffer from operational problems due to increased competition for available spectrum and their inability to operate within this constrained environment.[46] UAS must acquire the ability to operate in a spectrum-constrained environment to perform their various missions and to function fully as a NCW asset. The following section first provides brief insights on how DoD arrived at this dilemma and examines its associated operational implications. The analysis then focuses on several initiatives aimed at addressing spectrum problems within DoD; specifically, those efforts concentrating on better integrating UAS into the NCW arena.

Consistent with transformation objectives, DoD equips its forces with significant technological capabilities. Units now possess dramatically improved command and intelligence systems, wireless and satellite communications, and other technical systems designed to protect their forces and enhance operational performance. These military units have brought these new capabilities, which include commercially procured systems, to Iraq and Afghanistan and turned them all on. This electronic surge resulted in a massive grab for available frequencies–competing not only with U.S. and coalition military systems but also with civilian, host nation, and other governmental agencies.[47] In some cases, military systems could not operate or were degraded due to frequency interference. Despite extensive coordination by U.S. Central Command to ensure proper pre-deployment apportionment of frequencies, the scale and complexity of operations in Iraq has dashed any hope of resolving all spectrum conflicts. John Grimes, the DoD Chief Information Officer and Assistant Secretary of Defense for Networks and Information Integration, admitted that DoD did not fully anticipate the demand for spectrum in the beginning of the global war on terrorism.[48] As significant as this demand was in the early stages of the war, the need continues to soar with the introduction of additional UAS, wireless radio systems, weapons, and sensors used by U.S. and coalition forces.

To compound the problem, the U.S. is now engaging in a form of electronic warfare as part of an effort to defend against insurgency tactics that employ radio controlled improvised explosive devices (IEDs). To counter the threat of IEDs, the U.S has fielded an array of electronic jamming devices that successfully disrupt the signals enabling the IEDs, but also unintentionally jam U.S. and coalition systems to include radio links controlling UAS.[49]

UAS continue to fill significant needs and they are in greater demand as they demonstrate battlefield successes. However, with restricted flexibility to operate in a dynamic and spectrum-constrained environment, they impose severe planning limitations on their users. Simply stated, UAS cannot operate nor "plug" into the network without adequate spectrum resources – which makes their contributions to NCW questionable. How did DoD get into this predicament? To address this question, let us review two contributing factors. First, operational necessity to field quickly UAS led to design solutions that did not take into consideration spectrum limitations. Second, DoD failed to enforce spectrum supportability as criteria during traditional acquisition processes.

UAS components require frequencies to send and receive signals that control aircraft and transmit collected video, data, or relayed communications. Each of these signals operates within a portion of the electromagnetic frequency spectrum. National and international regulations apportion those bands for military, civilian, and emergency (etc.) use; bands of the spectrum contain unique technical characteristics conducive for certain functions. For example, certain frequencies travel greater distances or can transmit larger amounts of information. Given this technical reality, many military and civilian systems gravitate to common frequency bands. Thus, activating all of these systems in the same geographical area creates conflicts. For example, many tactical and theater-level UAS can operate only in the 4-8 gigahertz range, referred to as C-band. Unfortunately, this is also the same band used by numerous radar systems, satellite and troposcatter communications equipment, and aircraft altimeters. Additionally, certain tactical UAS are "hard-coded" to use limited frequency pairs that are also heavily used in civilian and other military systems, and in fact, are not available for use in some countries outside the U.S.[50] Fielding UAS quickly provided a much needed war-fighting capability, but resulting design limitations have created problems for the theater commanders. In fact, DoD has cited inadequate spectrum resources or interference issues as the direct cause for numerous UAS operational failures.[51] If UAS do not have access to adequate frequencies, commanders must also make difficult prioritization decisions or come up with alternative solutions. Fielding capabilities quickly sometimes requires a departure from traditional DoD acquisition processes, which often leads to unforeseen operational problems. However, what about those systems, to include UAS, that follow established DoD acquisition guidelines?

While this paper does not thoroughly review DoD acquisition policies and procedures, it is clear that acquisition regulations include "spectrum supportability" criteria to ensure that the designed equipment can function in its intended environment. However, a report released by the Defense Spectrum Office asserts that "Current methods for assuring that systems have spectrum access are poorly defined, too slow, subjective and inconsistent." This report goes on to claim that the acquisition community frequently avoids spectrum supportability requirements.[52] In the final analysis, UAS and other critical military systems are encountering operational problems due to inadequate spectrum resources due in part to problems within military acquisition processes.

As spectrum availability problems persist, both DoD and the UAS development community now recognize the scope and severity of the problem. Vice Admiral Nancy Brown, the Joint Staff J6, asserts that adjustments to DoD acquisition processes now require earlier spectrum supportability assessments. Admiral Brown goes on to claim that improved spectrum management tools and training within the Services will improve current integration problems and help prevent further spectrum-related conflicts.[53] The UAS development community is also taking steps to ensure their products can operate within spectrum constraints. UAS the TCDL enhance interoperability and therefore improve informational dissemination. TCDL also promotes efficient use of the frequency spectrum by providing UAS the flexibility to operate in a wider range of frequencies.[54]

In keeping with DoD transformation objectives as well as current wartime operational requirements, services develop and field UAS and other capabilities that use advanced communication, sensor, and networking technologies. In essence, the DoD has entered the early stages of executing NCW – and within this construct has revealed significant challenges. Access to frequency spectrum is a fundamental requirement for many of these systems; perhaps a requirement taken for granted by some product developers. Regardless, this issue continues to cause operational problems for theater commanders. DoD's continued emphasis on network-centric operations makes reliable spectrum access even more critical.[55] UAS serve many significant roles within today's joint, interagency, intergovernmental, and multinational operational environment with more possibilities on the horizon. All of these missions require significant spectrum resources. Without adequate spectrum, UAS cannot provide and disseminate invaluable ISR information and cannot provide an aerial communications layer to support the soaring demands of the common theater network. The issues identified in this paper are all interrelated, therefore, DoD should address each in a holistic manner.

Recommendations

Integrating UAS within the theater communications network has challenged deployed units as well as DoD leadership. Acknowledging the invaluable service that UAS provide as well as the severity of this problem , the military has several initiatives that address this challenge – several of which are mentioned in this paper. DoD's transformation efforts and future operational concepts envision a network-enabled force empowered with systems that provide enhanced situational awareness of the operational environment. To ensure that UAS function fully as a NCW asset, DoD leaders should consider the following recommendations:

1. The DoD should ensure the design and fielding of UAS is done in close partnership with those agencies responsible for building and sustaining the common communications network. In pursuing the benefits of net-centric operations, many military organizations develop systems that rely on common networking resources to function. Specifically, the organizations that design, field, and sustain UAS probably are not the same organizations charged with similar responsibilities for the communications network. Observing established architecture standards and protocols will promote interoperability, and the scale of UAS operations requires increased collaboration among the

joint and service-level communications communities. The goal of the communications network is to serve the needs of the warfighter which includes enabling those battlespace systems, such as UAS, that require network support. Likewise, UAS must interface with the common network to ensure efficient dissemination of their products. The DoD must establish these partnerships early in the product design phases and ensure they remain intact throughout the acquisition process.

2. The DoD should support the systematic development of an aerial communications layer to broaden network availability and increase network efficiencies. The demand for network capacity continues to soar. Each service is pursuing an aerial communications relay capability to address some of these demands. However, the DoD must ensure a coordinated approach to developing this capability by establishing and enforcing networking standards and protocols. The department must provide concepts for network management and network planning. Finally, the DoD should pursue an explicit High Altitude Long Loiter (HALL) capability as part of the aerial layer tier. Such platforms can provide communications coverage for hundreds of kilometers and, compared with other lower level UAS, they suffer less from line-of-sight, airspace, spectrum, and weather limitations.[56] While experimental HALL variants exist, DoD does not have an official HALL acquisition program.

3. The DoD should ensure that UAS can operate in an environment with limited availability of frequency spectrum. UAS roles and missions will only increase as necessity demands, and they will operate not only in isolated battlespaces, but also in highly populated urban areas as well as ad hoc military operating bases. As with many network-centric systems, the DoD must strictly enforce spectrum supportability benchmarks early in the acquisition process. UAS testing should occur in a spectrum-constrained environment often in the design phases; UAS should have the ability to reprogram to a wide range of frequencies as required. To increase the ability to resolve UAS as well as other spectrum interference issues, the department must develop management tools that provide real-time awareness of spectrum use and that populate a database to visualize graphically the frequency use within a given environment.[57]

Conclusion

The Department of Defense, and indeed other U.S. and international government and civilian agencies, have just begun to capitalize on unmanned aircraft systems. Successes in this endeavor may inspire the design of unmanned systems that operate on land and in water. The potential of these systems to serve is almost unlimited. However, putting these capabilities into operation requires a thorough understanding of the communications environment in which they must function. These systems, like so many other capabilities designed under the imperative of promoting network-centric warfare operations, generate requirements on the theater communications network.

To make the DoD's vision of NCW a reality, UAS and the "network" must cooperate. Achieving this goal requires fulfilling three mandates: UAS must achieve interoperability with the theater network and other adjoining systems to promote information dissemination efficiencies; DoD must support developing the UAS role as an aerial communications relay node to broaden network connectivity within the theater; and DoD must ensure that UAS can function within an environment that contains limited frequency spectrum availability. Certainly, the services can field net-centric "pieces and parts" that alone offer tremendous potential. However, the ultimate challenge remains interconnecting these systems to build a unified and networked capability that satisfies warfighters' demands. Several solutions indentified in this paper, such as WIN-T, TCDL, and OSRVT, indicate that DoD is addressing this effort. The successful integration of UAS within the theater network will be a measure of DoD's ability to field and sustain net-centric capabilities as articulated in their vision and transformation objectives.

Prudens
Futuri

Blue Force Tracking: Building a Joint Capability

Lieutenant Colonel Michael M. Sweeney
United States Marine Corps

Blue Force Tracking (BFT) capabilities have been heralded as critical in helping to build situational awareness (SA) on the battlefield. They have become an important tool in today's operational environment. Commanders at all echelons have complimented the capabilities that this technology brings and its importance as a joint force enabler. So important is the capability, that within the Department of Defense (DoD) alone the plan is to grow the number of devices from about 50,000 in use today, to over 250,000 by 2015.[1] This does not account for increased interagency and multinational partners in operations. Despite the importance of tracking friendly forces and the anticipated growth in this area, a holistic approach on how to proceed in the development of a true joint capability is lacking. The devices in use today bring various capabilities from a number of manufacturers, most of which are incapable of sharing the blue force data they generate with different platforms on a peer-to-peer basis. Technical solutions and procedures that allow for the exchange of BFT generated information have been developed, but the ability to see all device inputs on a common operational picture (COP) is proving to be a challenging endeavor.[2] This complicates not only force tracking and command and control (C2), but also critical tactical operations such as clearing fires.

The complexity of warfare, increasing reliance on technology, and realities of the joint environment highlight the need for a strategy that will allow for the development of a joint capability in this critical area. Failure to address issues that present themselves today in the form of policy, standards, infrastructure, procurement, and training will complicate efforts to leverage this technology in the future. This analysis will frame the issues at hand, evaluate available options, and offer specific recommendations for building a joint capability.

Clarifying Terms

To gain an appreciation of the challenges that exist, it is first necessary to outline the vernacular used when discussing BFT. The Chairman of the Joint Chiefs of Staff (CJCS) describes BFT as the "employment of techniques to actively or passively identify and track U.S., allied, or coalition forces for the purpose of providing enhanced battlespace situational awareness."[3] BFT devices generally can be categorized as one-way (beaconing) instruments that have the ability to send data only, or two-way instruments that can both send and receive "blue" and other data that provides a level of situational awareness as well as some ability to command and control.

One-way BFT devices simply determine **where** a friendly unit is located, and **who** the friendly unit is. The data used to determine where the unit is consists of time, latitude, longitude, and altitude information obtained from an embedded Global Positioning System (GPS) (this information can also be obtained from other position reporting systems). The GPS obtained information normally refers To Whom It May Concern: Position Location Information (PLI), and that, combined with pedigree information associated with the specific transmitting device is commonly referred to as a "track."[4]

Two-way devices generate this data as well, but also have the ability to provide **status** and **intent** information. Blue Force Situational Awareness (BFSA) is the collection and integration of capabilities provided by systems or tracking devices and transmission mediums employed to obtain, report, and share Blue Force Identification.[5] Situational Awareness is the coupling of situational development (interpreting the operational environment through all available input mechanisms) and situational assessment. Blue Force Tracker and BFSA contribute to situational development but not entirely, nor do they provide a full assessment of friendly forces or other elements that commanders must take into consideration.

Some have come to see BFT as a way to reduce fratricide. One could argue that BFT informs the Combat Identification (CID) process, but BFT devices are not designed to reduce fratricide as CID systems are.[6] BFT contributes to SA, and that coupled with target identification forms the foundation for shoot, no-shoot decisions that CID systems are designed to facilitate. Figure 1 shows the nested relationships between BFT, BFSA, SA, and CID.[7]

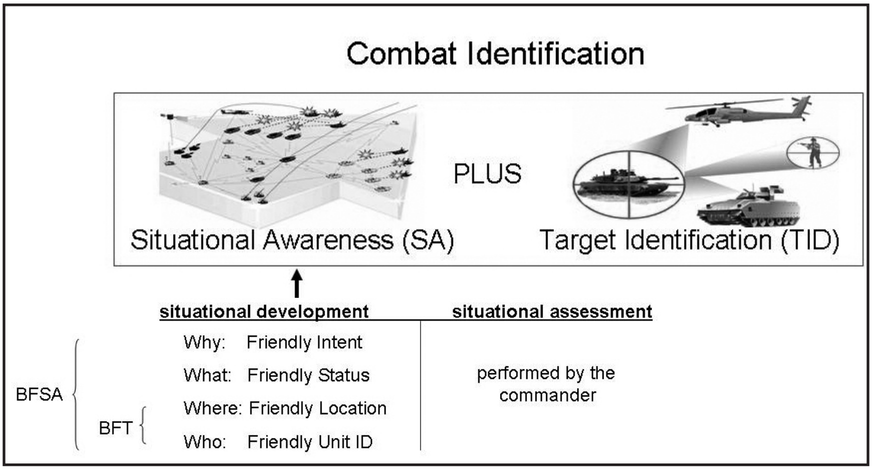


Figure 1

Although this analysis is not intended to evaluate specific tracking devices or systems, the various types and increasing numbers have in fact created interoperability challenges. Although most of the challenges have been highlighted through the extensive use of BFT by the U.S. Army, U.S. Marine Corps, and special operations units all Services, Combatant Commanders (CCDRs), and joint organizations share equity in overcoming the obstacles at hand. At least twelve different BFT/BFSA systems are being used in operations ongoing in Iraq and Afghanistan. This capability has proven to have applicability in virtually every functional warfighting area, but the majority of devices are segregated in such a way that they align with particular mission domains, or functions, and their unique operating requirements.[8] Brief descriptions are provided below.

Conventional force BFT systems generally provide BFSA capabilities to tactical forces. System displays plot a variety of markers on area maps including blue force positions and status, known red force positions, engagement locations, and comprehensive messaging capabilities. This can best be described as the digitized version of the hard copy maps with acetate overlays in combat operation centers of old. Conventional force systems are designed to operate in either a classified or unclassified mode.

Logistics BFT systems track logistics vehicles and containers using both one-way and two-way communications. They normally use commercial-based satellite services that operate at the unclassified level.

Special Operations Forces (SOF) and Other Government Agency (OGA) systems provide tracking of personnel, with an emphasis on secure Limited Probability of Intercept (LPI) and Limited Probability of Detection (LPD) tracking. This ensures that the location of SOF and OGA personnel are not compromised. The majority of these systems employ a beaconing capability associated with one-way communications and only limited two-way communications in the form of brevity codes. The communications architecture supporting these devices operate at the classified level.

Personnel Recovery (PR) BFT systems operate at the classified level and provide tracking and messaging to individual persons needing rescue. They are only used in the event that a rescue is needed and are not activated during missions by default. They are used extensively in the aviation community for pilot rescue.[9]

The alignment of functionality with mission domain makes sense from a requirements perspective provided the devices developed and procured are able to share data and information. That is not the case today.

The BFT System

A BFT system consists of more than just the tracking device. The system must include the position location and identification function, a transceiver, a communications network, and a user interface. Together these elements allow for the generation, transmission, processing, and display functions that vary according to Service, hardware, resource availability, and data handling policies and protocols. Figure 2 graphically depicts the functional composition of a generic BFT system and the steps required to allow certain disparate devices to share information.[10]

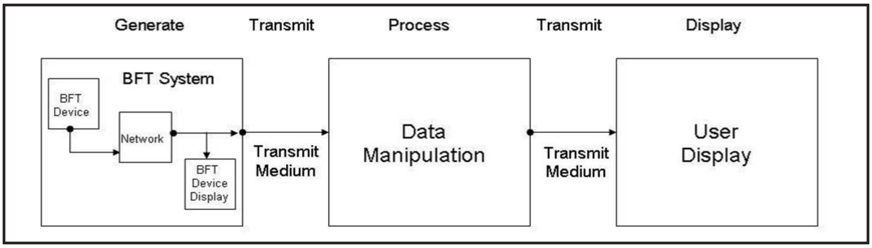


Figure 2

Some similar devices do have the ability to communicate on a peer-to-peer basis, as indicated within the first block of the diagram where the generate-transmit-process-transmit-display process still occurs. These closed BFT systems require further transmission and manipulation of data in order to be shared with dissimilar devices.

Based on the figure, one can begin to get a sense for the complex nature of the systems that take BFT data and translate it into information that is readily displayed and easy to understand. It is clear that BFT technology has significant utility, but the lack of fidelity in, and enforcement of, standards to ensure interoperability has created multiple stove-piped systems which cannot communicate with one another, forming the requirement for a joint BFT capability.

Challenges

As already mentioned, there are a number of devices within the DoD inventory that generate BFT data. Historically, the Services have been responsible for designing, procuring, fielding, and sustaining their own combat gear. This Title 10 responsibility serves the individual Service well by allowing the freedom to match desired capabilities with materiel solutions. This process was sufficient in the short era of joint C2 up to and including Operation Desert Storm, where combat actions were largely de-conflicted by space and time, and Service-provided forces were able to work together through greater reliance on analog processes and segregated operational environment.

Unfortunately, Service specific requirements and acquisition processes do not facilitate joint interoperability today. The Joint Requirements Oversight Council (JROC) was designed to address the issue of interoperability, but the initial guidance from this council was to converge existing BFT for ground forces vice develop a true joint capability.[11] Subsequent updates to the JROC have been focused on convergence only. Some progress has been made, but the task is proving more difficult than originally anticipated for a number of reasons.[12] Some are associated with technical challenges, while others are policy related issues that require difficult decisions that have yet to be made. The processes that support the JROC are prone to Service parochialism as positions are often based on program protection vice the best interests of the joint community. Consequently, the Services continue to procure devices that generate tracking information using different formats and various communication protocols.

It is also important to note that many of the devices now being used grew out of Advanced Concept Technology Demonstrations (ACTDs) vice programs of record within the Services. ACTDs are intended to exploit mature and maturing technologies to solve important military problems by allowing users to gain an understanding of proposed new capabilities for which there is no user experience base. Many devices in use today were originally provided to warfighters for evaluation.[13] They quickly saw the utility of this technology and the evaluations turned into extended operational tests that required additional devices easily procured through the ACTD construct. This got the capability fielded quickly by avoiding the normal acquisition process. Urgent Need Statements (UNS)[14] and the realities of a post-9/11 world added to this type of procurement by the Services to meet increased operational needs. Collectively, these factors have exacerbated the interoperability challenges faced today.

Once BFT data has been generated it has to be moved so that it can be manipulated into information that is useful to its consumers. This is commonly accomplished by injecting information into the common operational picture (COP) for theater wide distribution. Terrestrial based communications, like those provided by tactical radios, limit the range of communications and amount of data that can be passed. Although a few devices use this medium to transfer data, the majority use satellite-based communications that provide an over the horizon (OTH), on the move (OTM), beyond line of sight (BLOS) capability.

Military and commercial satellites, to include some originally designed for use only by some of our federal agencies, are used primarily because of their reliability, survivability, and BLOS communications. Not all the satellites used operate within the same frequency spectrum or classification level, which complicates the engineering of solutions. The heavy reliance on space-based communications as a transport mechanism also drives up operating costs when military satellites can not be used.[15] The utilization of commercial assets is high today, and with the expected growth in tracking devices, may prove excessive in the future without improvements in moving BFT data around the battlefield. Use of commercial systems also brings up the question of susceptibility and reliability of data transmitted, particularly when those service providers are foreign owned and operated, or when intermediary network operations centers are used that are outside the military controlled domain.

An Interim Solution

The realities described above generated a need to develop a capability that could collect the various forms of BFT data, translate that data into a format that could be widely used, and retransmit the data back to the theater from which it was generated at the desired classification level. U.S. Army Space and Missile Defense Command's Mission Management Center (MMC) in Colorado Springs has evolved from an organization originally designed to deal solely with BFT data collected by nationally controlled overhead assets, to one that can process data from all devices that generate BFT information on the battlefield today (provided adequate communication paths are in place). This is most commonly done by translating BFT data from the various devices in use into a format compatible with the Global Command and Control System (GCCS), more commonly referred to as the COP. The magnificent work performed by the professionals within this organization give commanders with access to GCCS the ability to see all BFT generated data within their area of operations.

This functional "BFT center of excellence" approach has helped to resolve many information exchange problems, but it does not completely fulfill the requirement for BFT data exchange at the lowest levels. If tactical users are not using devices that are compatible with the GCCS family of systems that normally reside at the Brigade-level and above, then they may not be able to see all devices within their area of influence.

Some argue that the cause for current interoperability challenges is lack of a single agency with direct budgetary authority over BFT system development. This may be partially to blame, but the proliferation of BFT devices can be traced to other historical reasons as well. First, no Service or CCDR truly anticipated the utility of these systems on the battlefield, which were developed to work with Service unique transmission and data distribution systems. Warfighters, policymakers, and contractors failed to recognize the impacts of digitization that started to take hold in the late 1990s and the implications of technology when fighting in a joint environment. Although a plethora of data related standards exist to help improve interoperability, there has been little directive oversight applied to enforce adherence to standards. Service specific development efforts, ACTD procurement, and the UNS answered immediate needs, but none were concerned with interoperability across the joint community, and focused only on compatibility within a Service or unique mission domain.

Operational need for BFT has risen exponentially since the onset of the global war on terrorism (GWOT). CCDRs, Services, and agencies have been pressing for more of these devices. This has created the need for solutions quickly, which has detracted from efforts to develop capabilities that are interoperable and joint. GPS and continued electronic advances have reduced both the time and cost of developing systems, which has in turn, driven their accelerated proliferation.

Future Requirements

Having briefly looked at the events that have transpired to date regarding BFT, it is now necessary to consider emerging requirements for the future before specific recommendations on how to proceed can be made. The projected growth of devices (250,000 devices in use by 2015) will only exacerbate interoperability problems if the current way of doing business is not immediately changed. One device will not be able to satisfy all requirements, but there is a significant need for reduction in the number of systems used. Having fewer types of devices would limit the various architectures and configurations and in doing so improve interoperability. The ability of devices or systems to intercommunicate automatically facilitates both efficiency and effectiveness.[16]

A reduction in the number of systems would also improve proficiency and training efforts. Although training is adequate for the individual device, users rely heavily on contracted Field Service Representatives (FSR) for maintenance and software modifications to the systems. Training in the use of a specific system is important, but we must begin to incorporate the administrative functions into our school house curriculums as the dispersed and complex nature of future operating areas may not allow for contractor support. Maintenance and sustainability would also improve dramatically with a focused effort on fewer numbers of systems.

Commanders have advocated for the ability to "see" all friendly forces operating in their Area of Operations (AO), and that information should be available on a single C2 display to assist in the decision-making processes. As the number of BFT devices and systems have grown, so too have the bandwidth and network requirements to support them. Some of these networks operate at the classified level to support BFT related missions; others work at the unclassified level. Some are designed to work with organic terrestrial based assets while more and more are migrating to satellite-based communications. These variations make it difficult for commanders to get a display that shows all blue forces operating within their AO without the service provided by the MMC. The reliance on this organization to build a comprehensive picture limits the operational flexibility of BFT.

The current National Security Strategy (NSS) and National Military Strategy (NMS) make it clear that the military must be prepared to operate in any clime and place. The ability to deploy and operate globally on short notice requires global coverage for the collection and dissemination of BFT data. Current communications architectures in place to support BFT systems can best be described as theater specific. They use overhead assets that are often only available in that region and most require movement through a systems-specific processing or network operations center prior to being sent to the MMC. A growing majority of the overhead assets and processing centers are civilian controlled and funded through contracts executed by program managers within a Service. This too limits the operational flexibility of many BFT systems.

A joint capability also requires a new approach in the collection and dissemination of BFT-generated information. Space power is a decisive, asymmetrical advantage for the United States, and especially for the U.S. military. But heavy reliance on overhead assets creates some vulnerability. While the United States will continue to dominate space in the near future, other nations and future adversaries are certainly not bystanders. Most potential adversaries study and understand U.S. capabilities, and strive to adapt technologies to overcome their own disadvantages. The United States must begin to explore communications alternatives that provide the OTM, BLOS capability desired by users within the BFT community.[17]

Information assurance of the BFT architecture is another critical requirement. There is a joint need for secured (safe) and ensured (guaranteed) communication among all friendly entities. There is also a need to ensure CCDR-controlled, unexploited access to BFT data. Network vulnerabilities that potentially provide enemy forces with this type of information must be guarded against at all costs.[18] Although the risk of exploited BFT data is low in today's operations, the proliferation of computers and ever-increasing computing power can arm potential adversaries with sophisticated tools that increase risk in this area. Technologically capable nations have conducted electronic attacks against the U.S. military and will continue to do so. The application of electronic warfare is a different sort of combat power which can be as lethal as kinetic fires to military and civilian targets. Computer and network attacks can reach across the world at the speed of light, invisibly targeting large masses of people in both military and civilian communities.[19] Their uniqueness requires well-considered policy as well as systems developed that can defend against attacks from packets of electrons.

The classification of the data itself plays an important role in designing the architecture to support the various systems. There is a significant policy debate ongoing within DoD regarding the proper classification of BFT data. Current interpretations of classification of data are being made from policies developed for the handling of hard-copy information routed via couriers. It is woefully inadequate in dealing with the technological advances made over the last few years in networking, communications, and electronics. The current policy development process is essentially a "political" activity, one in which the issues at hand require conciliation of diverse interests among the groups that have become identified with them.[20] This is particularly challenging as it relates to classifying BFT data because the systems were developed in a way to support the Service interpretations on the handling of data.

For example, the Army approaches the classification problem from the perspective of providing every soldier with a BFT capability in the future. Since it is an unrealistic endeavor to get every soldier a security clearance, they side on declassification of BFT data for users below the squad level. The Marine Corps believes that this data should be classified. They envision the use of both one-way (beaconing) to select individuals, and two-way devices located at key leadership positions, and view the matter of BFT information as one of disclosure that can be shared if the mission calls for it. The combatant commands believe that classification is mission dependent, but that it should be classified when engaged in combat operations.[21] Establishing a policy on the classification of BFT data is a fundamental issue in developing a joint capability. This policy will significantly affect concept of operations, distribution of assets, and network architectures to support BFT employment.

Data exchange between devices requires network compatibility. Services face a challenge in this regard as some radios and networks employ different sets of standards. Incompatible protocols and disagreements regarding what message standards to use are significantly hampering interoperability efforts. This reality has increased complexity to our Service networks as additional translation processes have had to be added in order to share information.

The current concept of operations, or lack thereof, coupled with the rapidly growing demand for BFT has implications for the larger, joint common operational picture. GCCS is the DoD joint C2 system of record for achieving full spectrum dominance. It enhances information superiority and supports the operational concepts of full-dimensional protection and precision engagement. GCCS is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture necessary to conduct joint and multinational operations. It is the heart of the COP. GCCS fuses select C2 capabilities into a comprehensive, interoperable system by exchanging operational and planning information to include BFT data.[22] The growing number of BFT devices alone could degrade the utility of the COP based solely on the volume of data they would produce if left unchecked. Common procedures must be developed and utilized to manage how BFT data is handled within the COP.

Recommendations

With BFT interoperability as the desired end-state, then success must come in the form of leadership, strategy, and resources. The recommendations that follow address each of these areas and offer specific actions for improvement and the development of a joint BFT capability.

The leadership framework is in place in the form of the JROC and supporting processes. As mentioned, the JROC focus has been on converging existing capabilities. As early as 2003, it became apparent that there was a need to improve efforts related to BFT interoperability.[23] Despite several JROC memorandums, limited progress has been made in reducing the variety of devices in use, or in sharing of data at the lowest levels. CJCSI 8910.01 provides Joint BFSA (JBFSA) operations guidance, but does little to define CCDR requirements.

Joint Forces Command (JFCOM), under the Joint Battle Management Command and Control (JBMC2) Roadmap, has established a JBFSA Executive Steering Committee (ESC). This organization is charged with providing leadership in developing combat effectiveness and improving interoperability and integration in this area.[24] They are currently focused on addressing previous JROC memorandums calling for the convergence of existing capabilities. Although this forum has forced compromise, it has not adequately addressed development of a joint capability. The ESC has limited ability to serve as a forcing function because members consist of Service representatives who naturally look to protect Service interests and investments. The committee has helped in identifying some of the more difficult issues for which decisions are needed, but has had limited success in forcing JROC decisions on them. Further hampering the JBFSA ESC effectiveness is the issue of Title 10 requirements versus CCDR needs.

A shift in focus is needed that will enable consideration of the critical issues at hand for a JROC decision. Such a shift would set conditions for enhanced interoperability in the future. Efforts should focus on the following:

- Breaking down the barriers of heterogeneous environments that include systems used by all military Services
- Developing a strategy for integration and interoperability developed from the merging of CCDR and Service requirements
- Building BFT infrastructure that supports all theaters, CCDR CONOPS, and anticipated growth across the joint spectrum

The first step in such an effort must be the development of a concept of operations from which a BFT implementation strategy could be developed and resources applied. Former Chairman of the Joint Chiefs of Staff, General Peter Pace, called for such an effort when he stated that, "The JROC should take a leading role in the formulation of CONOPS in order to help identify and fill gaps in capabilities."[25] This is important because although various BFT CONOPS exist that are Service or theater specific, none have been developed that address all mission domains across the spectrum of conflict in a joint environment. The Chairman went on to say that developing joint concepts of operations that will be used 10, 15, 20 years out will enable the development of systems that provide these capabilities.[26]

JFCOM should lead this effort for the JROC as their mission calls for them to provide interoperable forces, develop joint enabling capabilities, and to assist leadership in making proactive, informed decisions.[27] A CONOPS that incorporates the details needed to develop a joint capability would require input from each CCDR and Service, and should consider coalition and other government agency concerns. Each Service has estimated the number of devices required for their specific organization, but the concept of employment for these devices has not been synchronized.

JFCOM has done some work in the development of a joint CONOPS but the level of detail required to make policy and budgetary decisions requires additional technical expertise. A cadre of electrical engineers, computer scientists, and members of the MMC who have limited, or better yet, no habitual ties to any specific Service, is needed to augment JFCOM J85, who has done much of the heavy lifting for the JBFSA ESC. This small but skilled team should draw members from industry, the Defense Information Systems Agency (DISA), or systems engineering organizations from outside the Services.

This cadre could facilitate CONOP development by participating in the JFCOM led process with CCDRs and Services. Their expertise would serve to inform decisions regarding capabilities desired and how best to employ the technology. They could interpret and incorporate existing capabilities and concepts, and offer recommendations for how best to link requirements across mission domains. The technical focus of the cadre is needed to assist CONOP developers with issues such as device density implications to networks, security concerns and risks, and overhead resource availability. The expertise the cadre could offer would allow for the fidelity needed to identify additional issues requiring decisions and recommendations on capabilities required in a family of systems approach that meet CCDR and Services needs across all mission domains. There is no question that during this process some hard decisions will have to be made, as this approach will challenge Service positions and investments. The cadre could serve to inform the JBFSA ESC and JROC if required on such contentious issues, and should be available to the Services to explain certain recommendations and positions in an effort to belay any fears.

DISA, the Joint Staff J-6, and Department Chief Information Officers (CIOs) all have equity in the development of network and data communication standards. Despite the great work of the individuals within these organizations, the U.S. military still develops unique systems designed to work within Service schema and architectures. The continued Service-centric development of what should be inherently joint and interdependent systems will be totally inadequate for the future. Each Service will argue that their programs adhere to published standards, but the issue of real standardization lies in the fact there is no enforcement mechanism at the joint level. Today any Service can defend the interoperability of their programs by simply proving that they can communicate with GCCS via a habitual system relationship or through the MMC. In reality, GCCS does not reside below the Brigade-level and that is exactly where interoperability efforts must be focused. A better model would be a validating function that ensures interoperability at the platform level. This needs to exist outside Service purview and within the joint realm

The previously mentioned cadre plays an important role here as well. Their alignment within JFCOM, who is responsible for the development of joint C2 systems, would allow them to provide a Service independent technical assessment, enforcing adherence to standards and protocols by Service and other tangential efforts dealing with BFT procurement. If a proposed procurement aligns with the strategy and meets the technical parameters, it would be approved. This would help in another critical area in building a joint capability – governance. Providing recommendations rooted in adherence to technical standards at the platform level would leave little room for Service interpretation. This function becomes critical when moving from a position of trying to make Service developed systems work jointly to one that requires the systems to be born joint.

Equally important in this strategy development is the need for clear policy regarding the classification of BFT data. The fact that systems have been designed to work over an unclassified or classified network should not drive the policy. Currently, Service intelligence, information assurance, and information system experts are working this issue, and are considering a compromise where data generated from users below the squad level is considered unclassified and everything above classified.[28] This approach is short sighted as it is one that is based on current systems and will require additional protocols in the architecture to handle translations functions that complicate development and implementation efforts.

A policy must be developed that reflects the operational realities of warfare in the 21st century. Evaluating future threats and vulnerabilities to our devices, networks, and communications infrastructure will be required before any informed policy can be made. Policy should be developed from operational requirements and not from the difficulties associated with clearing all potential users or the ease associated with disclosing information. JFCOM should again lead this effort in providing the recommendation, with the JROC ultimately making the decision. Whatever the decision, it must be directive in nature to ensure joint standards are set and enforced.

A definitive policy on data classification can be worked in conjunction with a phased migration to network standards that would not only solve current BFT challenges, but interoperability on a much larger scale. Enforcement of adherence to a data classification policy could easily be incorporated into the function of the technical cadre within JFCOM. The recent call for a roles and missions review within DoD that advocates joint control of funding for command, control, computers, and communications assets presents the opportunity to enforce desperately needed governance in this area.[29]

Fiscal resources have not proven to be a challenge in procuring capability over the last six years, but this is likely to change in the future. A family of systems approach must be adopted to reduce the number of disparate systems currently being used to fulfill the same capability requirement. Requirements documents and contracts must be written in a way that forces interoperability. Currently, several of the devices used by DoD are produced by the same primary contractor, yet many of these devices are incapable of passing data on a peer-to-peer level. A single, family of systems contract is needed that places stringent demands on the product provider for adherence to predetermined standards and interoperability metrics. Senior leaders need to engage directly with the executives of these companies and be willing to cancel contracts if discrete interoperability metrics are not achieved. Services will argue that this approach is cost prohibitive and too time consuming, but this is in fact possible if program refresh schedules are synchronized in such a way that allow for incremental movement towards standards developed for a future BFT capability. The equipment refit issues that the Services face due to ongoing operations present an opportunity for new contracts to be written that could improve interoperability if done correctly. There would undoubtedly be a net savings in total expenditures by adopting a family of systems approach that could be re-invested to address remaining issues such as the need for systems administration training.

A five-fold increase in the bandwidth will be needed to support BFT devices over the next five to seven years.[30] The heavy reliance on space-based communications for BFT services creates some vulnerability in the form of limited capacity and commercial reliance that must be mitigated. Alternate collection means must be explored that allow for global response as called for in the NMS. Surrogate satellite technologies that are neither theater specific nor reliant upon commercial providers to operate must be explored. These expeditionary capable devices would mitigate much of our overhead reliance on space-based assets while improving our flexibility in supporting operations around the globe.

The Defense Advanced Research Projects Agency (DARPA) has been exploring such capabilities. Airborne Communications Node (ACN) is a DARPA program to design, develop, integrate, and demonstrate a prototype communications payload for airborne platforms. It can provide enhanced theater communications capability for on-the-move warfighters. This multi-function payload enhances and augments essential warfighter communication services. One of the target platforms for the ACN payload is the Global Hawk high altitude endurance unmanned aerial vehicle. Another such possible platform is the high altitude airship. ACN is not a unique, stove-piped communications capability. Rather, it enhances and augments the current mobile military communications infrastructure by working with it. It simply emulates the services that satellites currently provide. Multiple surrogates would be required to provide the same coverage area as satellites, but it could improve intra-theater communications and inter-theater reach-back, thereby reducing the reliance on overhead national and commercial assets.

The scalability of this capability is also an attractive feature as it could be used for a small Joint Task Force or for large scale operations. Units traditionally responsible for communications planning, installation, operations, and maintenance would manage these resources much as they do with current satellite-based systems. The senior communication organization would provide the linkage back into the DISA network. An important benefit of this technology is its ability to provide communications without the need for supporting infrastructure. It is self-deployable – at least to the extent that any airborne platform is. By loitering over the theater, it provides an instant communications capability for existing military radios on the ground, at sea, or in the air.[31] This approach could reduce the dependency on space-based assets and provide a mechanism for "theaterizing" the collection, and subsequent distribution of BFT data. It would also serve to simplify the communications architecture needed to support BFT and provide greater operational flexibility for commanders. Requirements to provide BLOS and OTH communications make it necessary to explore emerging technologies such as this. If properly resourced and considered today, it could alleviate some of our challenges and provide great operational flexibility in the future.

Conclusion

Throughout the centuries, three simple geographic location questions have been all-important to soldiers and leaders at all levels:

- "Where am I?"
- "Where are my forces and other friendly forces?"
- "Where is the enemy and what is the best route to attack him?"

Combat experience in Afghanistan and Iraq shows that BFT-equipped forces provide immediate and accurate answers to these critical location questions that have always been – and will always be – essential to decisive military operations.[32] So important is this capability that within DoD alone the military will experience exponential growth in the number of devices fielded between now and 2015. The variety of devices and different capabilities they provide have created interoperability challenges that directly affect the ability to exchange this critical data at the tactical level. These challenges will increase unless a joint capability is developed that can meet all mission set requirements.

A strategy developed with CCDR and Service input, coupled with informed and effective leadership and adequate resources will set the conditions to improve interoperability of this critical capability. Hard decisions will be called for, but the young men and women who will go into harm's way in the future deserve nothing less.

Providing an Enterprise Service Architecture to the Net-Centric Warfighter

Colonel David P. Acevedo
United States Army

> *At the end of the day, our warfighters really only want one thing – rapid and reliable access to the network, their data and applications from stable and unchanging computer configurations as they move from home station, through mission rehearsals, and into theater operations.*[1]
>
> —Commander NETCOM, MG Carroll F. Pollett

Evolving operational needs and the ability to share information across functional, organizational and unit boundaries remains problematic as identified in seven of the nine combatant commands Integrated Priority Lists (IPLs).[2] Recent experiences in Iraq and Afghanistan demonstrate the need for better cross organizational information sharing strategies that will guide the transition from today's information sharing paradigm to a net-centric paradigm.[3] The limitation in access to required information, collaboration and knowledge sharing capabilities is affecting commanders' abilities to gain true situational awareness in today's volatile, uncertain, complex and ambiguous (VUCA) operational environments.

Future combat forces must rapidly deploy into a theater capable of operating in joint and multinational environments while coordinating operations with other U.S. Government and selected civil organizations.[4] The ability to fight immediately upon arrival requiring little or no systems reconfiguration places increased demands on how the military designs and operates its networks. Theater operations will continue to be joint and multinational, resulting in the need for greater levels of cooperation and integration between U.S. forces, other Department of Defense (DoD) components, coalition, and host-nation organizations.[5] As military missions grow more complex, robust communications and network integration and interoperability will become increasingly vital to warfighting operations.

The DoD accelerated its transformation efforts following the terrorist attacks of September 11, 2001. These sweeping transformation efforts increased integration, interoperability, and focus on net-centricity greatly accelerating the transformation of Joint, Interagency, and Multinational (JIM) warfighting capabilities.[6] As a result, today's joint force is more expeditionary, modular and agile.[7] The reality of this transformation, as well as its operational requirements, demand emphasis on information sharing within and across organizational boundaries both at home station and when deployed.[8] Tactical and operational elements rely on networks to leverage strategic capabilities which allow them to deploy and fight upon arrival.[9] This complex operating environment demands that commanders have integrated network connectivity through an Enterprise Service Architecture (ESA) that provides immediate access to the network.[10] To achieve full integration and interoperability requires the continued expansion of the "joint team mindset" from the combatant command level down to the JTF and component headquarters.[11] Furthermore, the elimination of seams between functional components and within DoD will enhance this integration creating the ability to truly share information across time and space.

This paper examines current policy and guidance on the implementation of Active Directory (AD) and recommends a strategy that facilitates better integration of these architectures to provide enterprise-level services. This analysis provides a conceptual framework for providing shared access to enterprise-level resources, and an examination of the current Army AD policy as it relates to units in home station, their relationship with the Local and Area Processing Centers (LPC's/APC's), and the transition of tactical units away from home station into deployed operations. Additionally the strategy, guidance and policy for the development of a Resource Forest (RF) architecture that will work in coexistence with the current Army and Joint Task Force-Global Network Operations (JTF-GNO) AD architecture will be addressed.[12] The RF strategy provides enhanced integration that strikes the right balance between control, security, autonomy and flexibility while keeping the fundamental principle of "work and train as we fight." Separate Generating Force (GF) and Deployed Force (DF) Forests leveraging a common Enterprise Application Resource Forest (EARF) will provide for a consistent and acceptable secure means to host enterprise-level services and share them across a joint force providing net-centricity through a Service Oriented Architecture (SOA). Using this concept, the implementation of the EARF will minimize the need for systems reconfiguration and administrative coordination during the transition process as tactical units deploy in support of DF operations. The EARF concept minimizes security risk and allows for the greatest level of transparency, flexibility and integration for deploying units while ensuring continuity of operations and access to critical information and collaboration resources throughout all phases of operations.

Primer on Active Directory

Directory and Enterprise Services are key elements to the military and DoD networks providing the essential foundation to the theater network support infrastructure for access and collaboration.[13] All successful operating systems today work off of a core Directory Service (DS) that controls access to resources. At the component and enclave level, the primary DS supporting the joint forces and DoD is Microsoft's Active Directory product.[14] Active Directory is Microsoft's implementation of an international DS standard. In the DoD environment, AD forms the nucleus for all activities. This spans authentication, permissions, digital identity, online "presence" and the presentation of a Global Address List (GAL) through Exchange and state management. Active Directory provides for integration, increased interoperability and supports the Net-Centric Enterprise Service (NCES) architecture for the DoD and other governmental agencies. Active Directory also allows for the distribution, management and oversight of globally deployed Group Policies Objects (GPO) providing flexibility in maintaining the health of the network and enterprise services through the application of Information Assurance (IA), antivirus definitions and installation of new applications; all managed and deployed from a central point across the enterprise.[15]

In short, AD is the DS for many DoD components and is essential to the net-centric vision. To be net-centric, any infrastructure needs to provide a consistent identity, access, and policy enforcement foundation. Active Directory provides this foundation for access to Enterprise Services (ES) and is generally the accepted DS across the LandWarNet,[16] the DoD, and the Global Information Grid (GIG).[17]

Active Directory in the Modular Force

The United States Army created modular units that are self-contained, sustainable and organized with capabilities for the full range of missions that provide for better integration and interoperability to support the joint environment.[18] Presently, Corps, Divisions and Brigades operate and maintain their own Non-Secure Internet Protocol Router Network (NIPR)[19] and Secure Internet Protocol Router Network (SIPR)[20] AD Forest while in both the GF and DF environments.[21] These "multiforest"[22] structures do not inherently allow for the separation of domain enclaves of user accounts or exchange and enterprise application services outside of the same Forest structures. As a result, these multi-forest structures cannot easily share resources with one another.

The most significant advantage of the modular force is greater strategic, operational, and tactical flexibility.[23] Although this flexibility ensures the most effective support to the warfighter, it presents significant challenges to achieving and maintaining transparency, integration and security when designing and implementing the supporting AD infrastructures. As stated by Vice Admiral Nancy E. Brown,[24] "Active Directory was supposed to be a panacea. Well, the way we've implemented it, it's no different than what we've ever had before. We implemented Active Directory just like we've done everything else: We've done it by Service [sic], and there's no interdependence at all; in fact, there's little interoperability if you look at it."[25]

The Army's AD multiple Forest approach provides for separate Forests (A forest is a collection of every object, its attributes and rules in the AD. The AD Forest, tree, and domain are the logical parts of an AD network) that can operate autonomously in support of units operating in deployed theaters of operations.[26] This multiforest approach allows for units to exercise full operational control for all assigned AD Forests and equipment at the expense of providing a secure shared Area of Responsibility (AOR) based resource environment.[27] Within this environment interconnected Brigade Combat Team data networks operate autonomously during the early phases of an operation. They then operate interdependently when able to connect in a theater capable of providing enterprise-level support and services. The transformation towards systems of interdependence while maintaining the capability of modular units to operate independently will increasingly require data architectures that provide access to enterprise applications and services in the deployed environment and at home station. It is this necessity for autonomy and interdependence, while maintaining operational and tactical control that must remain consistent as the DoD moves forward with its NCES concept and provides for the seamless transition of tactical units from GF environments away from home station into combat theaters of operations. As the 16th Chairman the Joint Chiefs of Staff states when addressing the capabilities of joint warfighting and transformation: "Joint warfighting …it is a prerequisite to winning the War on Terrorism and will significantly accelerate and be accelerated by transformation. This will require collaborative and innovative solutions to difficult cultural and resource challenges. The future joint forces must transition from an interoperable to an interdependent force where different capability sets can be rapidly integrated to achieve desired effects."[28]

Using the NETCOM Concept of Operations (CONOPS) for Implementing AD in Tactical Army Units, defines an autonomous unit as "any unit that satisfies the Joint Expeditionary Mindset (Task Force Modularity) and can be deployed without regard to any habitual relationship or Task Organization CONUS or otherwise."[29] Within these units (Corps, Division, and BCT's) consists a single AD Forest structure and a single AD domain.[30] As a result, to share information across Forest and domain boundaries requires the establishment of a "meshed" architecture that makes it difficult to define the authoritative sources of information and requires an inordinate amount of administration and coordination overhead to gain coherence in information and knowledge sharing. Using this meshed architecture by establishing "trust relationships" during the pre-deployment and deployment phases, requires the Enterprise Administrators for each Forest to coordinate with all other units that are part of the deployment to set the deployment architecture and establish a series of "transit trust" between each.[31] This is necessary to ensure the sharing of information and is in compliance with DoD Directive Number 8320.02, dated December 2, 2004, that states, "Data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification. Data that is accessible to all users in the Department of Defense shall conform to DoD-specified data publication methods that are consistent with GIG enterprise and user technologies."[32]

For tactical Army units to share information seamlessly across Forest boundaries requires the establishment of a series of AD trust relationships. However, in the deployed force environment, trust relationships are only permitted between DF Forests that are task organized (headquarters and sub-elements assigned, attached, or OPCON) for deployment or training. Trusts are not permitted between DF Forests that are outside the same task organization.[33] This prevents the establishment of a net-centric and enterprise service architecture required to share information throughout the force.

Using the RF concept, the data architecture for a theater of operations consolidates enterprise level services at the JTF, theater or regional level, greatly reducing the number of required AD trust relationships. This enables future forces to move from independent and autonomous operations to a more interdependent force where capabilities and the desired effects are achieved (no change) through the integration of systems across the force.[34]

Challenges and Observations OIF 05-07

During Operation Iraqi Freedom (OIF) 05-07, within the Iraq AOR, there existed no less than 27 separate Army tactical AD Forests. It should be noted that there are more than 200 in the tactical Army AD structure and more than 40 in the CENTCOM AOR presenting significant challenges to integration, transparency and security.[35] This situation limited the ability to access and share information across

Division, Brigade and Corps Forest boundaries. Seamless access to governmental agencies and units from other military Services was even more problematic requiring intense administrative coordination and account duplication resulting in users needing multiple accounts and logons. The Corps was responsible for installing, operating, and maintaining three separate data networks that included NIPR, SIPR and the Combined Enterprise Regional Information Exchange System (CENTRIXS)[36] for email, collaboration, Voice Over Internet Protocol (VoIP), video-teleconferencing, SharePoint and Command Post of the Future (CPoF). Lack of unity in the joint AD structure created problems in every security domain. This made it difficult to replicate GAL, as well as developing consistency in the application of security related group policies necessary for centralizing configuration and management from the enterprise level. The situation was further complicated by limited bandwidth to the Brigade Combat Teams located in Forward Operating Bases (FOB's) as well as inadequate knowledge of operating enterprise Information Technology (IT) services to include Microsoft AD.[37] As a result, the AD architecture created a "disjointed" information sharing environment causing commanders to stovepipe information impacting the ability to synchronize efforts to achieve the desired effects. A unified AD structure would have lead to better synchronization while enabling net-centricity and easing system administration thus allowing for access to information and collaboration while increasing mobility for the warfighter.

Introduction to the Resource Forest (RF)

The basis for the RF discussion requires the understanding of the following:

1. The DoD Network-Centric Enterprise Services (NCES) is not yet fully implemented
2. The establishment of the Local and Area Processing Centers is not yet completed
3. The Army will continue transformation requiring self supporting modular units
4. The GIG is not fully mature to support tactical unit reach back for access to enterprise level services[38]

5. Forward deployed tactical units will continue to operate within their own AD Forest structures at home station and when deployed
6. The continued requirement to interoperate in a joint environment with other Services and DoD organizations and the equipment they bring to the fight

A large theater network ensures continuity of information to incoming organizations and enables units to "fall in" on an operational IT infrastructure – achieving mission readiness on the first day in country through rapid integration.[39] The need for immediate access to resources and the ability to collaborate across the force is a fundamental war fighting requirement. Supporting tactical systems must seamlessly integrate becoming interdependent as a Theaters Information Grid (TIG) matures. Tactical units must be able to deploy from home station into any theater of operations with limited or no systems reconfiguration or disruption of service. This essential requirement represents an expected level of service and data interoperability between tactical units. The Army's multiforest approach is the best AD topology supporting the modular force and the integration of the GF into DF operations. The multiforest approach allows large organizations, such as the Army and DoD that have multiple modular units and supporting organizations to deploy separate AD structures as it provides for the greatest level of autonomy and security.[40] The RF topology is a supporting multiforest configuration that is used for hosting application services and is supported as part of the CONUS GF AD architecture.[41]

The concept of an EARF is not complex. Simply put, it is a separate Forest that hosts enterprise-level applications that are available to all organizations either deployed or in a supporting GF environment. Users who need access to these enterprise applications authenticate through their own AD Forest structures and gain access to resources and services that reside within the RF. It is this architecture that allows for a common "hosting" of services at the enterprise level that provides for sharing and access across the force while ensuring the proper standardization, security and configuration management in support of the net-centric architecture.

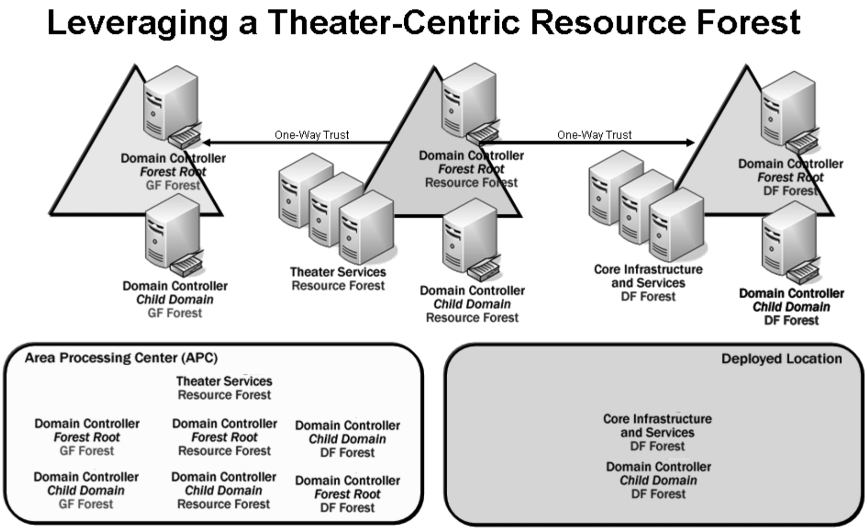


Figure 1[42]

The RF Forest is a "hub and spoke" architecture that provides for a "non-meshed" infrastructure that greatly reduces the administration (at the tactical level) and coordination overhead required when sharing information across multiple Forest boundaries. The EARF concept allows tactical units to leverage strategic resources while maintaining mobility on the battlefield which enhances information sharing. The same is true when autonomous units are at home station; access to resources are shared (no change) by both the GF and DF user base by establishing a separate Forests to host enterprise level services that can be accessed by both. For example, this is particularly useful for a Corps Headquarters under transformation (see Figure 1)[43] that supports a Main Command Post (MCP), an Operational Command Post and the Early Entry Command Post (EECP). Under this structure, much of the planning and support is derived from the MCP at home station and forward to the OCP and EECP. As a result, all CP's can now access a common enterprise structure hosting a set of services that is separate and distinct from the Forest structure supporting the MCP for garrison operations. This greatly reduces the security risk of extending the garrison Forest structure into a combat theater of operations by placing essential enterprise services into separate Forests that are extended or deployed with an OCP/EECP.

The Theater Network Architecture

Although recent progress is evident, interoperability remains an elusive goal that the U.S. military and the DoD continues to fight on many fronts.[44] As observed by the Multi-National Corps – Iraq Commander in 2005: "In Iraq, battle command spanned the full spectrum of joint and coalition war-fighting concerns, to include policy differences on how we protect our data networks through information assurance, service differences on networking and collaboration, the standards necessary to implement active directories, and our ability to share information in a complex architecture."[45]

The network-centric force is structured around concepts of Knowledge Management (KM) that requires constant access to information and people. This requires an extensive, standardized, interoperable and well protected enterprise service architecture that provides continuity of information, ease of access, and the ability to provide the right services to the right location at the right time. The theater network architecture applies "jointness" to systems engineering, design, planning, deployment, and operation of enterprise information services.[46] As joint forces are increasingly networked, linked and synchronized; dispersed forces are able to better communicate, share information and collaborate.[47] NETCOM's long-term objective end state to achieve this is to provide the tactical portion of the Army Enterprise Infostructure (AEI) by extending the network and access to enterprise services (NCES) from Army component commanders in a GF environment to deployed forces supporting a joint, combined, or single-service task force conducting expeditionary operations.[48] Until this vision is realized, DF forces must have access to key resources resident in a theater of operations while maintaining their modular flexibility to deploy and integrate into theater network centric architectures.

NETCOM establishes that while Brigade Combat Teams (BCTs) are at home station, they will leverage LPC/APC enterprise services through the installations networks via the establishment of Virtual Local Area Networks (VLANS) and through the Joint Network Nodes (JNN) when training using the Regional Hub Nodes.[49] Deployed forces will access enterprise level applications and resources via reach-back through Standardized Tactical Entry Point facilities (STEP)[50] or

Teleport sites to an APC location.[51] It is this architecture that allows for the centralized management of services that requires incorporation into DF architectures forward and available immediately upon arrival into theaters of operations. As stated by the CENTCOM J6 when addressing a panel on Joint Task Force JTF interoperability, "Operational information, data, knowledge sharing requirements exceeds the ability of the existing infrastructure. Data management strategies and Tactics, Techniques and Procedures (TTPs) are needed to disseminate and stage information forward in support of the Warfighter at the first tactical mile."[52] As stated, it is a warfighter requirement to stage information forward. In order to accomplish this the best approach is achieved by applying the principles of an Enterprise Service Architecture forward in the fight.

Trust in a Multiforest Approach

The Army's AD multiforest approach decentralizes the operations and maintenance of its directory services to tactical units.[53] This provides for the greatest level of autonomous operations while presenting significant challenges to administrators and the ability to share information and collaborate across AD Forest boundaries. To allow users in one domain to access resources in another, AD uses Forests and trusts.[54] The Forest concept simplifies both end-user access to the directory and management of multiple domains. Using the multiforest approach, all domains and trees in a Forest inherently trust one another for the purpose of authentication.[55] Such trusts do not extend automatically between Forests, which requires directory administrators in modular units to manually configure trusts between Forests.[56] This is necessary as Microsoft defines the security boundary for AD Forest enclaves to reside at the Forest level.[57] This is also necessary as the availability of enterprise applications and collaboration services such as SharePoint, databases and applications specific to Communities of Interest (COI) require tactical units to authenticate users across Forest boundaries. As a result, for tactical units to authenticate users within their own Forest structures and gain access to resources in other tactical Forests requires coordination and "trust" relationships between participating organizations. This is problematic for deployed forces as trusts between

DF Forests outside the same task organization is not authorized thereby limiting access to shared resources.[58]

Presently, the Army alone supports more than 140 tactical Forests within its tactical AD architectures.[59] In a theater of operations such as Iraq, and to share information and collaborate with every other Forest owner, requires the establishment of multiple separate AD trust relationships each requiring written approval by the DAA.[60] Without these trust relationships, units cannot easily share information and collaborate across their Forest boundaries. Although trust relationships in themselves are not problematic, the management of these relationships requires intensive administrative oversight and directly affects the ability to maintain transparency and seamless integration into a Theater Information Grid (TIG) immediately upon arrival. As an AOR is typically transitional in nature, units are constantly rotating in and out of theater requiring them to reestablish trust relationships with other rotating units to ensure total access.

Security in a Multiforest Architecture

The necessity to establish AD trust relationships between Forest owners requires a level of security that is common throughout the DoD.[61] The AD Security Technical Implementation Guide (STIG) provides security and standardization configuration guidance for the implementation of Active Directory within the Department of Defense. The STIG's design assists System Administrators (SAs), Information Assurance Managers (IAMs), Security Managers (SMs), and Information Assurance Officers (IAOs), with the implementation of AD configurations and is intended to provide a certain level of security compliance assurance.[62] It also allows for individual sites to determine the level of assurance that is appropriate to their environment and mission.[63] Experience demonstrates that organizations do not always adhere to the security guidance established by their component service or within the DoD. As a result, this creates a level of "mistrust" between Forest owners and prevents the establishment of a cohesive and robust information sharing environment. To alleviate this mistrust, units must be required to validate their AD environments during their Mission Rehearsal Exercises (MRE's) in accordance with the policies and guidance provided by the DOD and their supporting combatant command. As previously mentioned, validation of all AD structures will ensure the ability of deploying units to seamlessly integrate into a combat theater of operations and ensure the required access to key resources and applications.

An Examination in the Successful Implementation of a RF

The ability to dynamically collaborate and share information requires an architecture that provides services that are immediately available and easily accessible to units in transition and within a theater of operations. The deployment of the RF in Iraq is an example of an ESA that provides theater level services supporting forces in a highly mobile environment.[64] In the Iraq Theater of Operations (ITO), to establish information sharing between modular unit Forests and the theater Forest requires one of the following:

1. Establish individual accounts on the hosting theater account domain
2. Establish trust relationships between users supporting Forest account domains and the theater Forest domains

It is important to note that the establishment of this trust only allows for the sharing of information between these two Forests. The following are advantages and disadvantages of RF architecture model:

Advantages

- Provides for enterprise data sources that can be managed centrally or through a shared administration model. Provides net-centricity
- Reduces the need to migrate information to incoming and outgoing units thereby easing access to information
- Supports modularity while reducing the administrative burden
- Can be grown into a regional or theater resource capability
- Provides for better integration & access to information across organizational boundaries

Disadvantages

- Creates an additional Forest at the enterprise level
- Requires enterprise administration oversight
- Requires organization to change their culture to share information
- Requires additional infrastructure
- Added complexity to develop the initial design
- Requires corporate "buy in" for this non-traditional approach

Multiple Accounts on Multiple Domains

Without AD trust relationships between unit domain structures, individual accounts must be created in the hosting account domain. This creates the need for multiple accounts and log-ons across multiple security domains. This presents a significant security challenge as external users can not be positively identified and abuse of user accounts and passwords becomes evident (Figure 2).

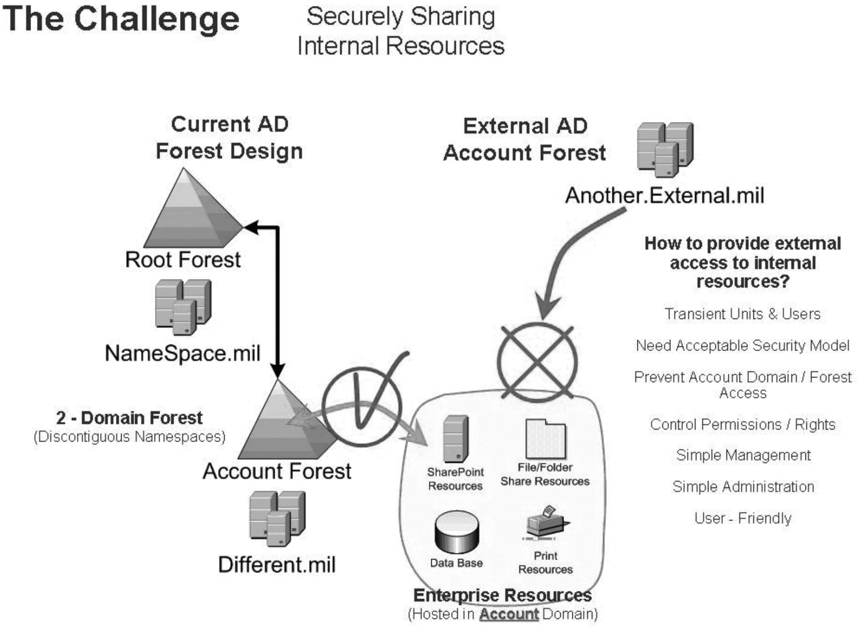

The Challenge
Securely Sharing Internal Resources
Current AD Forest Design
Root Forest
NameSpace.mil
2 - Domain Forest
(Discontiguous Namespaces)
Account Forest
Different.mil
External AD Account Forest
Another.External.mil
SharePoint Resources
File/Folder Share Resources
Data Base
Print Resources
Enterprise Resources
(Hosted in Account Domain)
How to provide external access to internal resources?
Transient Units & Users
Need Acceptable Security Model
Prevent Account Domain / Forest Access
Control Permissions / Rights
Simple Management
Simple Administration
User - Friendly

Figure 2[65]

To eliminate this vulnerability using the RF architecture, users authenticate through their supporting account domains inherent in their modular AD Forest structures.[66] This provides the mechanism whereby an organization hosting enterprise-level services can accept that external users are authenticated by a trusted partner and can grant them access without having to be responsible for managing their identity information. Within this framework, users enjoy seamless, secure access to enterprise services and multiple applications. This not only simplifies the process of granting access, it also makes it possible to maintain the high levels of security necessary to protect the integrity of that access.

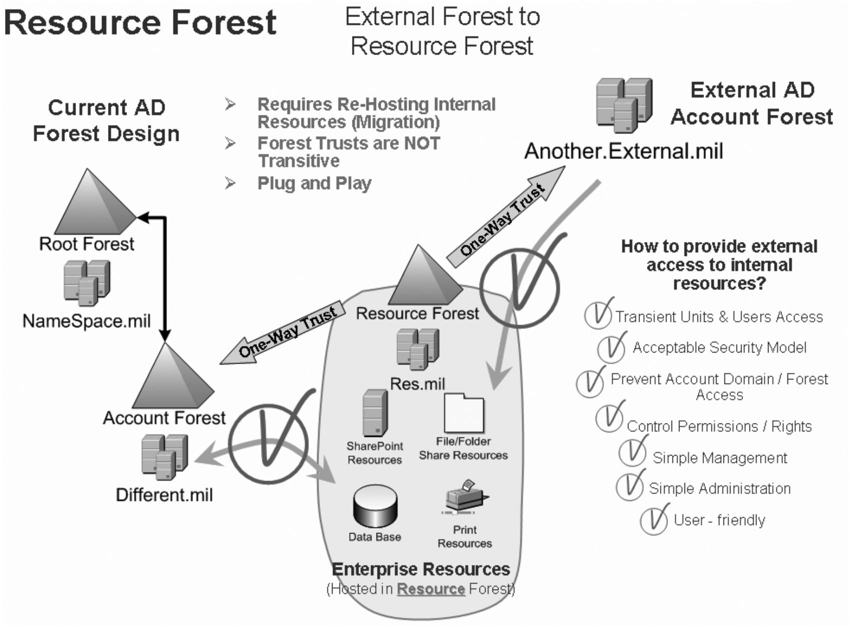

Resource Forest
External Forest to Resource Forest
Current AD Forest Design
Requires Re-Hosting Internal Resources (Migration)
Forest Trusts are NOT Transitive
Plug and Play
External AD Account Forest
Another.External.mil
Root Forest
NameSpace.mil
One-Way Trust
One-Way Trust
Resource Forest
Res.mil
Account Forest
Different.mil
SharePoint Resources
File/Folder Share Resources
Data Base
Print Resources
Enterprise Resources
(Hosted in Resource Forest)
How to provide external access to internal resources?
Transient Units & Users Access
Acceptable Security Model
Prevent Account Domain / Forest Access
Control Permissions / Rights
Simple Management
Simple Administration
User - friendly

Figure 3[67]

Providing Resource Access

The correct method of providing access to shared resources is to create domain local groups in the RF and assign access rights and permissions to those groups.[68] Then access to resources within the RF is easily managed by adding domain global groups (or individual user accounts) from external domain(s) to the domain local groups in the RF. Since this method uses domain local groups in the RF, those groups are restricted to the RF. In other words, domain local groups can not be used external to the RF so it is not possible to transfer them or their members outside of the RF structure.[69] This method of providing external access to hosted services is under the complete control of the hosted service's administrative account(s) within the RF. This allows administrators for a hosted service to fully manage access and security for their services and resources. This architecture provides for the greatest level of unit control for unit applications with no assistance needed from RF Administrators.

Flexibility

The RF Forest topology provides for the greatest level of flexibility and allows for the ability to rapidly affect change in the operational environment. As previously described, the current tactical implementation guidance for AD requires Forest owners to establish trust relationships with every other Forest owner. This limits the organizations' flexibility as they often re-task organize or have changes in mission requiring trust relationships to be broken then re-established under the new task organization. A single trust relationship to an EARF limits the amount of coordination and administrative overhead while greatly increasing the continuity of operations and information sharing capabilities, regardless of task organization. The RF architecture also provides flexibility by using the shared administration model between enterprise administrators and the resource owners. Under this concept, resources are hosted within the RF structure and maintained by the owning organization. It provides for premier support as the DF can leverage expert resources when hosted within the LPC/APC or at the highest levels within a DF theater architecture. Because the RF is a shared administrative model, users can host services within the RF domain structure maintaining unit control and access.

Transparency

Transparency allows for access to the resources a war fighter needs to accomplish missions while deployed or in garrison. Currently, forces cannot quickly deploy IT services as large amounts of resources are spent creating and disabling accounts for end users that move from one geographical location to another or from GF to DF environments.[70] Tactical Forces are not able to move about an AOR quickly gaining access to systems, enterprise applications or a common GAL as Forest-level trust between units remains fractured.[71] Without an enterprise-level architecture for access to key resources, units only operate within their own information domains with limited or no access to theater-level information or collaboration services. In the RF architecture, all hosted services are managed individually and permissions to resources are managed by group memberships or individual user accounts from any trusted external domain. Units gain increased mobility by accessing a single enterprise resource Forest where all information is shared between multiforest owners. This approach greatly reduces the number of required trusts between Forest owners and minimizes the administrative and coordination requirements.

Standardization

For AD to interoperate efficiently, the DoD must adhere to a set of standards across the GIG. Active Directory inherently requires trust relationships to share information and collaborate between Forests and domains. Adherence to standards as determined by the DoD will minimize the problems associated with "mistrust" between Forest owners. However, adhering to standards is not enough; tactical AD structures must be exercised and evaluated during the pre-deployment stages of operations to ensure their ability to integrate into the TIG upon arrival.

People and Organizations, Changing the Culture

The greatest challenge to gaining net-centricity is changing the cultures of the participating organizations. As the DoD moves from an interoperable force to a more interdependent force, organizations are increasingly challenged to share information within and across organizational boundaries. To achieve this requires organizations to adopt the joint team mindset and willingness to share information openly. Forces must design their supporting AD structures not by Service but instead by standards set by the joint community at large. The DoD vision describes a future state where transparent, open, agile, timely, and relevant information sharing occurs that promotes freedom of maneuverability across a trusted information environment.[72] To achieve the vision requires organizations that encourage, and incentivize sharing; achieves an extended and available enterprise; strengthens agility to accommodate unanticipated partners and events; and ensures trust across organizations.[73]

Final Recommendations

It is clear that AD policies and strategies must increasingly address the need to share and collaborate across organizational boundaries to include those agencies within the Department of State, the DoD, and other governmental organizations. The development of a SOA founded on the principles of transparency, interoperability, and work as we fight while maintaining the flexibility necessary to operating in today's complex environments is required. Until the Army's Warrior Information Network–Tactical (WIN-T) and NCES programs are fully realized, tactical units require an architecture that allows for the seamless deployment from home station into a combat theater of operations with the ability to quickly gain access to key resources and applications. One conceptual way to accomplish this, and how the Army is currently doing this in Iraq, is to establish a separate RF for the hosting of key services and applications. This concept consists of multiple AD Forests with a shared Forest domain managed at the regional or theater level. This concept provides for faster deployment as it decreases organizational complexity, maintains unit autonomy while providing for interdependence, decreases the number of log-ons required by people who reside outside in their own tactical Forest structures and maintains an acceptable level of security risk.

To provide an Enterprise Service Architecture to the warfighter in today's net-centric environment, the following recommendations are for consideration:

1. Place key enterprise services and applications in separate AD Forests at the JTF, Theater or regional level
2. Develop a SOA that limits the number of AD trust relationships required to support the sharing of Information
3. Enforce and validate standards that promote interoperability and information exchange for all deploying units and organizations
4. Maintain a culture of jointness and information sharing by designing and implementing data architectures that focus on joint warfighting capabilities

Conclusion

The disjointed Forest structure that has emerged out of programmatic decisions, and the lack of trust, leads to an architecture that does not promote or establish the open sharing of information and collaboration across the DoD. The DoD and the Army must establish a data architecture that allows users spanning multiple domains to efficiently and reliably manage information and gain access to key resources. Access to common enterprise level resources and services is significantly improved using the EARF model.

The DoD NCES will be essential to implementing a network-based information environment that provides for increased information sharing and collaboration thereby enabling decision superiority. It will offer the core enterprise services based on Communities of Interest that will provide for common access to centrally hosted resources accessible through the GIG. Until this vision is realized, DF and supporting organizations must have access to resources and services that are shared across organizational boundaries at home station and where deployed.

The concept of a RF is slowly gaining ground and is being explored by NETCOM as a solution to better enable the warfighter. Recently, NETCOM hosted an "RF Summit" to determine the validity of the concept. Although additional technical details still need to be developed, the concept of the RF will "eventually solve many of the problems associated with access to resources in environments supporting multiple Forest."[74]

Prudens Futuri

Achieving the Department of Defense's Network Centric Vision of Information Sharing while Overcoming Cultural Biases to Control Information

Captain Paul M. Shaw
United States Navy

> *We cannot solve our problems with the same thinking we used when we created them.*
>
> —Albert Einstein

As a component of United States national security strategy, information sharing plays a prominent role in improving senior-level decision making by enhancing situational awareness and contributing to actionable intelligence. Toward this end, the United States Executive Branch and numerous government agencies, including the Department of Defense (DoD), Office of the Director of National Intelligence (ODNI), Department of Homeland Security (DHS), and Department of Justice (DoJ) incorporate cross departmental information sharing strategies into their respective operating practices. Each of these agencies' strategies mandates change for their respective corporate cultures from one of a "need to know" to that of a "need to share" in order to promote information sharing objectives. These mandates for culture change are strong with broad, encompassing objectives. Why then does the Government Accountability Office (GAO), along with other oversight agencies, find the United States Government (USG) lacking in its ability to achieve desired effects?[1] The fact that cultural impediments remain to implementing information sharing strategies is a key problem. As the 2007 U.S. Army War College Key Strategic Issues List (KSIL) suggests, achieving "…DoD's netcentricity vision of ubiquitous access in light of the cultural biases among people and organizations to control information" remains a core issue.[2] A key consideration is whether DoD can change policy and develop collaboration capabilities in order to promote information sharing and overcome cultural bias as it relates to controlling information.

Reviewing DoD's information sharing policies, in concert with examining various ways and means, provides a method for both clearly understanding the issue and determining appropriate courses of action. Policy change could potentially serve to promote net centric enablement and achieve desired information sharing effects. Policy can fail if it ignores Einstein's advice as quoted above by using the same thinking that created the problem to solve the problem. Policy failure may also result if there is conflicting policy guidance for the implementer to resolve. An example is the DoD's Net-Centric Data Strategy (NCDS), which articulates sharing of all information "except where limited by law, policy, or security classification."[3] The conflicting guidance found in the NCDS requires modification to clearly discourage cultural biases toward the control of information that limits information sharing. The DoD can then leverage the rules of successful cultural interaction and develop collaboration capabilities to overcome such bias. Another option is to consider alternative "means," in the form of capabilities associated with evolving technology, to counter cultural bias.

This examination of the DoD information control problem uses the U.S. Army War College (USAWC) strategy model of "ends, ways, and means," where: ends equal objectives; ways equal concepts; and means equal resources.[4] It explores the information control problem in terms of the scope of objectives (ends), policies (ways), and technology (means). In the USAWC Strategy Model, reducing objectives can help to achieve a balance between ends, ways, and means. However, since United States national security strategy and information sharing documents show a progression of desired information sharing capabilities, desired ends allow little latitude in reduction of information sharing objectives. Either modifying policy or using better technology is an effective strategy to achieve desired effects and to reduce risk. Tim Berners-Lee, founder of the World Wide Web (WWW), said, "It is essential that policy and technology be designed with a good understanding of the implications of each other."[5] This paper finds that changing ways and means are viable options for understanding and addressing DoD's cultural biases as they pertain to information sharing. The USAWC Strategy Model helps to determine if modification of ways or means is the better strategy for improved information sharing.

Policy

United States national security strategies display a range of information sharing objectives. These include the following:

- *The National Security Strategy of the United States of America (*NSS) uses information sharing as a way to improve intelligence and its use.[6]
- *The National Strategy for Maritime Security* (NSMS) strives for "full and complete national and international coordination, cooperation, and intelligence and information sharing among public and private entities."[7] Specifically, the NSMS argues for information sharing by calling for "timely, credible, and actionable intelligence" as an enabler for "situational awareness and integrated command and control."[8]
- *The National Military Strategy to Combat Weapons of Mass Destruction* includes guidance for information sharing in the mission thread for stopping WMD proliferation.[9]
- *The National Strategy for Information Sharing* combined with specific agency sharing strategies, such as the *DoD Information Sharing Strategy*, *United States Intelligence Community Information Sharing Strategy*, and *LEISP: United States Department of Justice Law Enforcement Information Sharing Plan*, are among a series of information sharing strategies designed to achieve these objectives.

The combined set of security strategies and information sharing strategies creates a framework for desired USG information sharing objectives. Of particular note is that the desired objectives (the ends) of these strategies continue to grow in scope and importance. Consequently, reducing ends may be the least acceptable option to bringing policy in alignment with objectives.

DoD Directive 8320.2 "Information Sharing in a Net-Centric Department of Defense" and DoD Directive 8320.02-G "Guidance for Implementing Net-Centric Data Strategy" are the core policies that promote data accessibility. Information assurance (IA) is a key aspect of policy espousing data accessibility. Department of Defense directives on information assurance such as DoD Directive 8500.1 "Information Assurance" and DoD Directive 4630.5 "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" promote IA in tangent with the goal of enhancing data accessibility. To further promote data accessibility, DoD Directive 8320.2 states, "It is DoD policy that: …data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification."[10] DoD Directive 8320.02-G provides "for governing and managing the development of new data sharing capabilities."[11] Its key contribution revolves around making data visible, accessible and understandable, along with promoting trust.

The information assurance requirements spelled out in DoD Directive 8500.1 for DoD IT systems runs counter to the Department's data accessibility objectives. "This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response."[12] The issue is further complicated by DoD Directive 4630.5 which ensures interoperability of IT systems throughout the DoD. This directive states, "IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare."[13]

DoD Directive 8320.02-G uses Communities of Interest (COIs) as collaborative user groups who "exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange."[14] COIs are responsible for developing data architecture within a particular context. In DoD Directive 8320.02-G, COIs identify authoritative data sources (ADS) which are further described as "data assets that are authoritative sources for data."[15] Data producers, who are members of

COIs, have the responsibilities to "make data assets accessible using web-based approaches."[16] This amalgamation of COIs, ADS, and data producers found in 8320.02-G is more about data structure, assets, and accessibility. It does not adequately communicate the responsibilities that data producers should have to share information. It is especially unclear with respect to authoritative data producers and does not help to diminish the cultural bias to control information.

Requirements for privacy, access, and ownership come from tasks, processes, laws, and policy. The Privacy Act of 1974 is an example of a law that imposes requirements on information exchange. The Privacy Act regulates the government's collection, maintenance, use, and dissemination of information on people. Its goal is to protect individual privacy rights of United States citizens and permanent legal residents. Under the Privacy Act, agencies must ensure that records with privacy information are accurate and complete. Agencies have a responsibility for allowing individuals access to their records for review of information.[17] Privacy information can require special validation processes to ensure accuracy, timeliness, consistency, and completeness, such as reconciliation keys and specialized metadata.

The Federal Information Processing Standards (FIPS) 199 is entitled the "Standards for Security Categorization of Federal Information and Information Systems."[18] FIPS 199 is a government-wide framework for understanding the risk of undesired information disclosure or system breach, which incorporates security categorization for information and information systems. FIPS 199 promotes analysis of the following risks: a security breach; adequacy of security objectives; and determination of a security categorization. This combination facilitates assigning the risk impact level of information and system compromise. Impact level could range from minimal effect to embarrassment to hostile response as they relate to balancing confidentiality, integrity, and availability as part of the FIPS 199 security categorization. The combination of the impact in connection with information classifications helps to determine the overall security categorization. These categorizations correlate to the organization's mission, legal responsibilities (such as the Privacy Act), asset and people protection, and threat considerations.

Given the stated objective, it would seem that the intent of the NCDS' policy to "share all" would transform the DoD culture from a "need to know" culture to a "need to share" in one simple stroke. Yet this policy allows wide implementation interpretation since it includes the statement, "where limited by law, policy, or security classification," and as evidenced by FIPS 199 provisions and other information assurance requirements.

Yet the tension between information assurance and information sharing are not the only problem. The current NCDS policy that articulates an information sharing strategy does not adequately address DoD's cultural biases among people and organizations as they relate to controlling information. Across DoD policies, the ability to implement information access has wide latitude for interpretation that creates tension between competing requirements. Allowing this interpretation has not worked for achieving information sharing objectives due to cultural biases at the organizational and individual levels. In this regard, the DoD NCDS uses similar thinking to cause and solve the problem in violation of Einstein's advice. The DoD NCDS accommodation of "where limited by"[19] enables culturally biased information control. This paper presents options for policy change with a recommended course of action.

Department of Defense's Cultural Biases

While there are many different definitions of culture, the following frames this evaluation:

> *A set of values, symbols and rituals shared by the members of a specific firm, which describes the way things are done in an organization in order to solve both internal management problems and those related to customers, suppliers and the environment....Culture manifests itself at both a visible level (age, ethnicity, gender, dress, organizational structure, symbols, slogans, etc.) and an invisible level (time, motivation, stability vs. change, orientation towards work, individualism vs. collaboration, control, how management views IT, etc.).*[20]

Precise agreement on culture's definition, however, is less important than examining and understanding organizational and individual biases manifested through culture.

There are cultural biases between organizations, where the respective cultures have to interact with each other. A cultural bias could be a result of an organization's responsibility to protect certain types of information due to either legal, moral, or agency mission requirements. Organizations have a fear of misuse of their data, sometimes with severe external consequences. Competition between agencies can create a cultural bias, especially when forced to work with each other. DHS, for example, in attempting to unify capability across 22 distinct agencies,[21] experienced the issue of developing points of integration and revision in support of interdepartmental information processes. In contrast, melding agencies is a common mistake when agencies start sharing common organizational purpose and goals, instead of determining points of integration and responsibilities for information sharing. This melding tendency may force agencies into trying to preserve understood relationships or their "homorphisms" ("A structure-preserving relationship between two sets of things.").[22] In such cases, a false sense of agency loyalty can impede use of other agency information. Similarly, legacy information technology systems also contribute to culture issues. When legacy systems have to undergo a modification to accommodate information sharing, organizations potentially create unintended conditions for resisting change.

Individual bias against information sharing reflects a variety of issues. For many, their bias regarding information control could be due to a desire to hoard information for reasons of power, influence, importance, job security, and reward. Creating products without collaboration can stem either from the lack of ability to collaborate or from systemically imposed resource constraints. Individuals may have problems electronically sharing products due to limitations of legacy systems. Some organizations have controls in place to ensure only final versions of products are available and prevent individuals from sharing developmental or draft product versions. Increasingly individuals experience information overload due to the volume of available information. Something that further compounds cognitive processes is the natural temptation of an individual performing a task is to seek out additional information until information overload exceeds their comprehension limits. Either an individual reduces available information and succeeds, or is overwhelmed. Many previous DoD information sharing efforts were dependent upon personal relationships, with skilled and experienced people knowing how to work around the system in order to get the right answer.

Individual and organizational risk aversion reinforces DoD's cultural bias for controlling information. Criticism or punishment is normal for the individual or organization deemed to inappropriately share due to a legal, moral, or classification issue. Rarely is an organization or individual punished for not sharing information. Even in the thorough reviews of major events like 9/11, proving an organization or individual should have shared information is difficult.

"When efforts to implement change fail, a common cause is insufficient attention to the people-side of change.... Treat information as a resource (on par with human resources, financial resources, physical resources) and consider how they can change the organization's information culture first through the people-side of change."[23] A starting point for the "people-side of change" would be respecting cultures, acknowledging cultural biases, and developing more effective policies and technology. Respecting culture could embody many things at both organizational and individual levels. Some of the best rules for promoting information sharing come from the following rules for successful cultural interaction by Professor Carlos Cortés of the University of California, Riverside.

1. Draw upon the strengths of diversity in order to work toward common organizational goals
2. Create a climate in which members of the organization feel welcomed to draw upon their diverse cultures and experiences, without feeling obligated to constantly represent "their people"
3. Draw constructively and flexibly on knowledge about groups, while using that knowledge as a clue, not as an assumption about individuals

4. Distinguish between those problems that can be resolved by establishing a rule and those that will require long-range, continuous action to modify attitudes, perceptions, and behavior
5. Accommodate constructively to diversity while also determining which accommodations are reasonable and which need to be limited
6. Work toward both equality and organizational effectiveness by determining when it is appropriate to treat all people alike and when it is appropriate to treat them differently[24]

Adaptation of these cultural interaction rules for information sharing is a potential key enabler of the required DoD culture change. Key constructs in these rules are to deal with organizations as entities, respect the rights of individuals in United States laws and understand organizational responsibilities. Successful information sharing would: work towards common organizational goals; respect personal and privileged information; work with groups without stereotyping individuals; understand when policies and processes will promote sharing responsibilities; allow for reasonable accommodations both for organizations and individuals; and understand when organizations and individuals should be treated alike and when they should be treated differently.

Allowing organizations to define how they should interact and their points of integration is a good way to adapt the DoD NCDS and other information sharing policies. Information ownership, access control, classification, privacy issues, and data quality attributes are information sharing requirements. These requirements create a context for information sharing and information availability, even if they are not comprehensive. As organizations capture and manage these requirements, they enable culture change conducive to information sharing. Some excellent work in commercial geospatial information management regarding transportation and real estate illustrate this principle of information sharing requirements management.[25] Understanding information related legal, moral, and classification requirements are a great way to promote information sharing and reduce information disclosure issues. Tim Berners-Lee advises, "Human communication scales up only if we can be tolerant of the differences while we work with partial understanding."[26]

The Technical Solution

Technology is a possible means for DoD culture change. Technological progress in processing speed, greater connectivity, and language compatibility enables great information sharing capabilities. Complex mathematics and logic use vast data stores and a multitude of sources through continually improving processing speeds and language understandable by machines. The evolution of the World Wide Web (WWW) into the Semantic Web is one of the best places to concentrate a focus for the type of technical solutions that can change DoD culture and affect information sharing objectives.

Evolving WWW technology offers a structure where the linkage and proximity of words would reveal patterns for development of context and understanding of meaning. The Semantic Web, Tim Berners-Lee's follow-on to the World Wide Web, changes data such that computers could learn enough to process machine-readable data.[27] Figure 1 illustrates Tim Berners-Lee's construct for the architecture of Semantic Web.

Current technology has different processes for how a person retrieves, uses, and stores data. These differences can affect the manner in which individual bias influences information control. The Semantic Web blurs the differences between these processes. This blurring starts with the Rich Description Framework (RDF) triplet concept of subject,

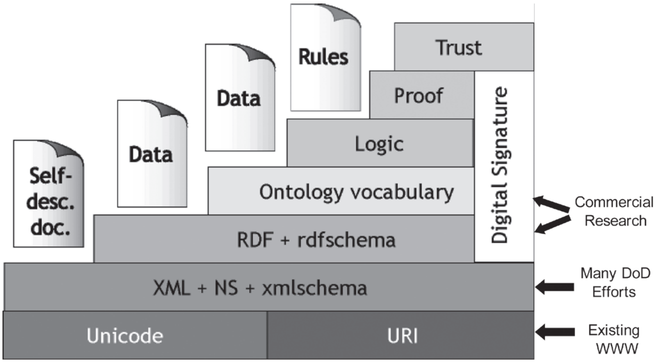


Figure 1: Illustration by Tim Berners-Lee at http://www.w3.org/2000/Talks/1206-xml2k-tbl.[28] The author added the annotation on the right side.

predicate, and object. Context will increasingly be instantiated with taxonomies, schemas, metadata tags, rules and constraints, and with properties and classes through ontologies. Ontologies make language machine-understandable. "Perhaps the most important contribution of the Semantic Web will be in providing a basis for the general Web's future evolution. The consortium controlling the World Wide Web had two original goals to maintain "interoperability" and "evolvability."[29]

In DoD cultural biases, technical issues of system interoperability, collaboration, and information sharing appeared as organizational and individual issues. An over-arching data architecture or single standard for the government to define intended use and promote exploitation does not exist nor should it exist. Tim Berners-Lee advised, "…making global standards is hard. The larger the number of people involved, the worse it is. In actuality, people can work together with only a few global understandings, and many local and regional ones….The minimalist design principle applies: Try to constrain as little as possible to meet the general goal."[30] Information has characteristics, such as dynamic (in a state of transformation from a process or task) or static (transformations complete and at rest) and public or segmented, that may prove a range of solutions that need to be pursued. Figure 2 shows that different quadrants appear with different solutions in each

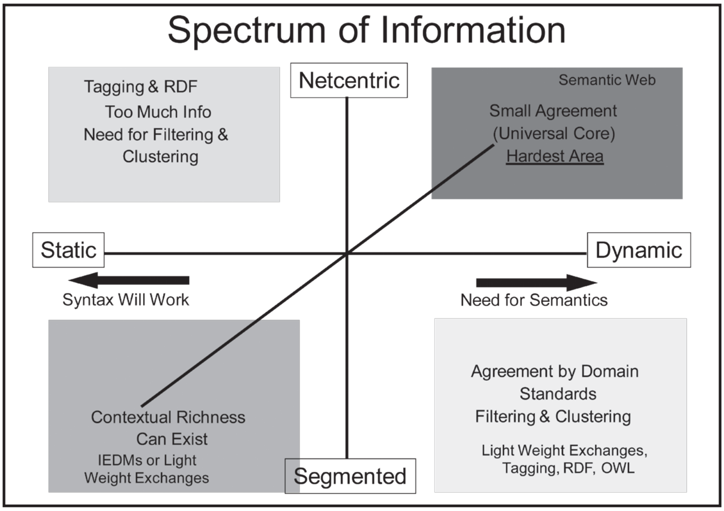


Figure 2: Information Spectrum – Even a basic classifications of the information illustrate that different strategies may exist depending on characteristics.

quadrant. There may not be one technical solution, but instead a need for a series of solutions in the different regions.

A key assumption in agency information sharing strategies is that key data has organizing constructs discoverable within a given context. Mission or task is an organizing construct for information classes, properties, and rules in the DoD. For example, the *Intelligence Community Enterprise Architecture Data Strategy* states, "…data are currently created and maintained to support the specific business processes that individual organizational elements are responsible for executing."[31] Development of context is a key concept for desired information fusion and dissemination in the future. Context most likely exists in layers (see Figure 3) developed over time with most information not achieving the top context layers.

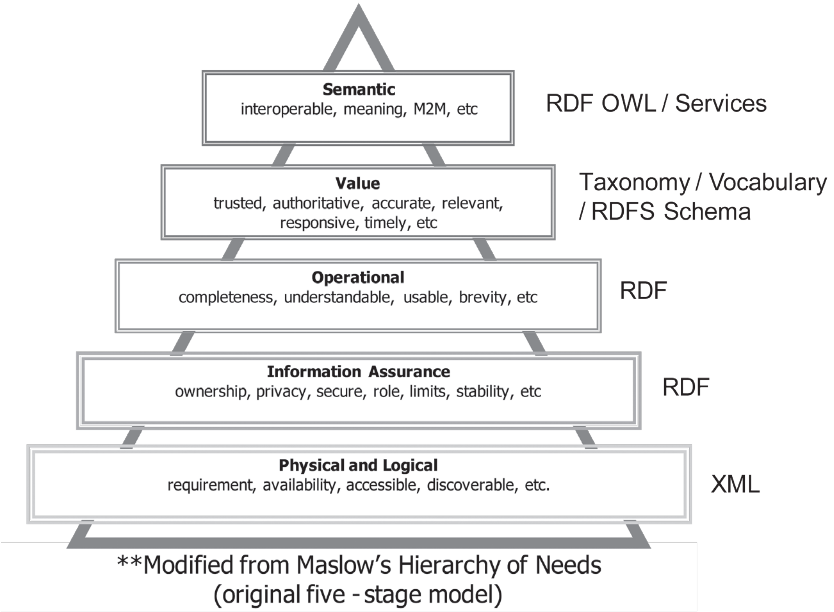
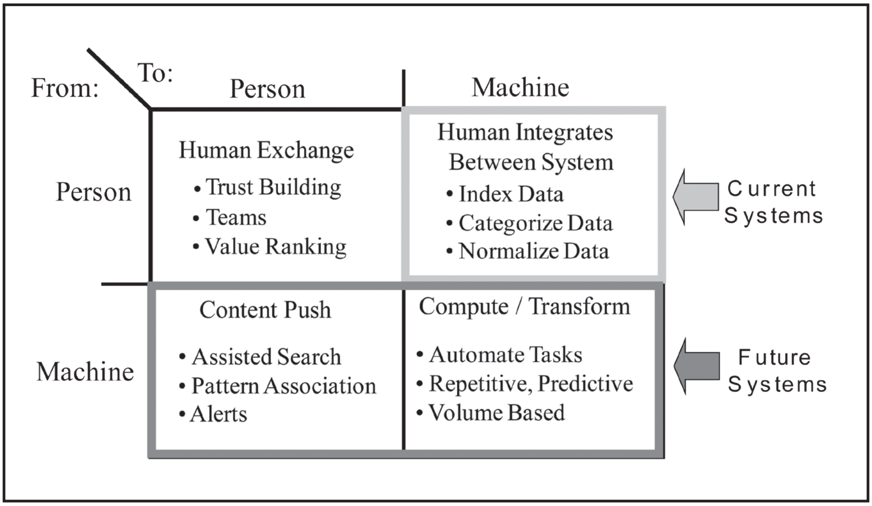

Semantic
interoperable, meaning, M2M, etc
RDF OWL / Services
Value
trusted, authoritative, accurate, relevant, responsive, timely, etc
Taxonomy / Vocabulary / RDFS Schema
Operational
completeness, understandable, usable, brevity, etc
RDF
Information Assurance
ownership, privacy, secure, role, limits, stability, etc
RDF
Physical and Logical
requirement, availability, accessible, discoverable, etc.
XML
**Modified from Maslow's Hierarchy of Needs
(original five - stage model)

Figure 3: Context Hierarchy – These context layers are adapted from Maslow's hierarchy by Tim Martin and Paul Shaw. The author presented this concept at the 2006 Systems and Software Technology Conference in a brief called "Semantics of Security."[32]

Many of DoD legacy systems either prevent or inhibit information sharing with others. Current information sharing integration points, such as DHS's Homeland Security Operation Center (HSOC) for terrorism information,[33] place complex burdens on smart operators to fuse information between multiple systems. Humans are often required to find, fuse, and retype key information between systems. Semantic technology offers many opportunities for better interaction for either machine to person or machine to machine, as illustrated in the following simple two by two grid of information flow in Figure 4.



From: \ To:	Person	Machine	
Person	Human Exchange • Trust Building • Teams • Value Ranking	Human Integrates Between System • Index Data • Categorize Data • Normalize Data	Current Systems
Machine	Content Push • Assisted Search • Pattern Association • Alerts	Compute / Transform • Automate Tasks • Repetitive, Predictive • Volume Based	Future Systems

Figure 4: Information Flow Grid – Most legacy systems are at the level of Person to Machine. Future systems offer Machine to Person and Machine-to-Machine capability. Dr. Dave Roberts and the author initially developed this grid. Minor modifications to the published grid are in this paper.[34]

As machines enable collaboration, people will accept new ways of collaboration to include machines dynamically creating teams among members who may never meet. This dynamic is easier for younger generations to accept, especially those who have grown up with chat and text messaging as acceptable social interaction. While collaboration tools enable improved information sharing, implementing the NCDS "share all" as a cultural issue is easier for those who accept this social interaction. A wise way to proceed is to understand when evolving technology requires human behavior changes and which groups are more accepting of those changes.

As the DoD continues progress towards net centricity, breakthroughs in information management and data transformation will occur. However, an over-dependence on technology is misguided and may postpone culture change. Melvin Conway stated,"Someone someday will find a better one to do the same job. In other words, it is misleading and incorrect to speak of *the* design for a specific job, unless this is understood in the context of space, time, knowledge, and technology."[35] If the DoD is not careful with new technologies, it will overwhelm users with information and negatively affect achievement of desired information sharing objectives. For the near future, all government agencies are dependent upon the human and their interaction with systems. Progress in assisting users with information and knowledge management is dependent on understanding how to assist humans and not overwhelm them during this transformation. General Pace, former Chairman, Joint Chiefs of Staff, stated, "I cannot yet tell you what transformation is. I am comfortable with the idea that if we had no new toys and we simply changed our mindset that we would transform significantly."[36]

Options

The following three courses of action examine the range of possible options between status quo, change in ways, and change in means.

I. *Maintain the status quo.* Continue allowing the data producer to define what to withhold in the posting of all data. Allow an ongoing tension between information assurance and information sharing. The status quo works with sensors and data sources with commodity type information, since they provide a bias for control or hoarding. Current DoD policy allows users wide latitude in deciding what they can withhold due to data confidentiality and integrity requirements. Users in their roles and responsibilities self-determine acceptable information control. Information control is most apparent when crossing organizational boundaries and less apparent within an organization. The current DoD environment has information sharing between systems and within processes. This option requires no changes to policy or additional resources, but lacks the ability to overcome cultural biases toward control of information, which is a question of strategic importance. Option 1 is not a viable option to achieve United States national security strategies or national information sharing strategies.

II. ***Formalize information sharing requirements with roles and responsibilities for data producers and process owners.*** Formalization would impose information sharing responsibilities on process owners and data producers, especially authoritative sources. This option is preferable for key operational data sources, especially designated authoritative sources. It promotes development of information quality attributes and data profiles. Formalization imposes responsibilities and control at key integration points to overcome cultural biases. This option allows for compliance monitoring and compliance should be part of the policy change. Existing Defense Information Systems Agency (DISA) technology and systems could perform automated compliance monitoring for the registration and production of profiled information products. Role and responsibility formalization could assist to overcome organizational cultural bias and overrule user discretion for withholding information. The revised policy creates a context to understand requirements for data availability, integrity, and confidentiality. Key operational nodes as data sources could transition to registered services to information sharing for the undefined user. Option II changes the existing NCDS policy to formalize information sharing responsibilities of process owners as data producers. It circumvents the existing policy of "post all data" and is most effective if key processes are targeted. This option follows the advice of Christopher Baum, Gartner Research Group, for how the government can effectively share data. Mr. Baum advocates, "understand where the data originates," "understand the law," and "find common needs."[37] Option II promotes information sharing effects through policy change, formalizing the sharing responsibility of data producers at key operational points and does not require adoption of new technology. Information sharing responsibilities with compliance monitoring overcomes individual information control biases.

III. ***Determine data sharing responsibilities of data sources.*** Technologically enable process owners with the ability to push information with a Semantic Web enabled context. Use the Semantic Web layers to enable user information markup and promote collaboration by tasks for self-synchronization. Determine integration points between organizations and develop common information objects for sharing. Formalize information sharing responsibilities of static data and allow semantic technology to tag data for control access. Allow user control of dynamic data, with posting at particular points of completeness as versions. Allow individuals to enter sharing agreements and participate in information exchange within the construct of task through machine-assisted collaboration. Use key processes at integration points with data sharing responsibilities to post available information as services with standardized metadata tagging and registered services. Process owners are aware of their information sharing responsibilities as with Option II. A key issue with Option III is the development of semantic technology and people with the technical skills to implement semantic layers. While pockets of excellence for semantic technology exist with communities like the medical community, the adoption of Semantic Web principles and practices is still evolving. The commercial market needs to develop collaboration tools to manage information and promote sharing to blur the division between information processes for retrieval, use, and storage. This Semantic Web is most likely a key evolution for the WWW and DoD Net-Centricity. The issue for the DoD is the immaturity of many elements of Semantic Web technology (refer to Figure 1) and the lack of trained people. The less risky option is to allow the technology to mature in the commercial sector and then transition to the DoD to provide information sharing capability.

Recommendations and Conclusions

A recommendation to adopt Option II and work towards Option III is the best strategy to address DoD's cultural biases and enable a culture change. Option II addresses the issue of information control directly and imposes sharing responsibilities on organizations and individuals by task and process. With the monitoring of information output at key integration points, policy compliance is checked. Technology can be an enabler for information sharing, but concentrating on technology will allow organizations and individuals to circumvent sharing responsibilities. Instead, an emphasis on Option II avoids the issue of technical maturity and transition from legacy systems. Pursuing Option II creates immediate effects and a way to build out in a modular implementation. As semantic technology is developed and implemented in the WWW and DoD's systems, Option II only becomes stronger. An over-emphasis on technology creates another excuse to delay behavior modification and effect change.

Using the USAWC strategy model of "ends, ways, and means," changing the DoD's NCDS and other policies is an immediate and effective way to counter DoD's cultural bias for information control. Additionally, it overcomes information control through determining responsibilities of data producers and assigning key operational nodes with sharing responsibilities. It also facilitates the monitoring of data producers for their compliance with the type and frequency of data products. Within this context, understanding requirements of ownership, access, classification, and other data quality attributes enables requisite understanding in support of information sharing, instead of playing into cultural biases for information control. In an increasingly complex and interdependent world, this policy change is required for effective joint, interagency, and coalition information sharing. Formalizing information sharing responsibilities will require addressing numerous technical and managerial information challenges as well. Likewise, consideration must be given to the technical challenges of exponentially growing volumes of data, developing proper information context, and promoting accessibility and discoverability of existing information that will be with us for years. Understanding a balance of the human, policy, process, and technology is critical for implementing a future vision of information sharing, as "it is essential that policy and technology be designed with a good understanding of the implications of each other."[38]

Prudens Futuri

Endnotes

Preface

1. Reagan, Ronald. National Security Decision Directive 130 (The White House, Washington DC: The White House 6 March 1984) http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm (accessed 23 December 2005).
2. Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as "Instruments of Power." It further states that Information, while not an instrument of power, forms a backdrop as all activity has an informational backdrop.
3. Neilson, Robert E. and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.
4. R.S. Zaharna, "American Public Diplomacy in the Arab and Muslim World: A Strategic Communication Analysis" (Washington, DC: American University, November 2001) http://www.fpif.org/pdf/reports/communication.pdf (accessed September 25, 2007, p. 2.
5. Groh, Jeffrey L. and Dennis M. Murphy, "Landpower and Network Centric Operations: how information in today's battlespace can be exploited," NECWORKS, Issue 1, March 2006.

Section One: Information Effects in the Cognitive Dimension

Mass Media Theory, Leveraging Relationships and Reliable Strategic Communication Effects

1. Richard Halloran, "Strategic Communication," *Parameters* (Autumn 2007): 4-14.
2. Werner J. Severin and James W. Tandard, JR., *Communication Theories*, (White Plains NY: Longman, 2001), 110.
3. Ibid., 153.
4. Ibid., 154.
5. Steven Curtis, Robert A. B. Curris, and Marc J Romanych, "Integrating Targeting and Information Operations in Bosnia," *Field Artillery*, (July/August, 1998): 31.
6. Melvin L. DeFleur and Sandra Ball-Rokeach, *Theories of Mass Communication*, (White Plains NY: Longman, 1989), 146.
7. Ibid., 164.

8. Ibid., 278.
9. Defleur and Ball-Rokeach, 279.
10. Denis McQuail, *McQuail's Mass Communication Theory*, (London: Sage Publications, Ltd., 2005), 476.
11. Ibid., 290.
12. Ibid., 293.
13. Ibid., 280.
14. Mari K. Eder, "Toward Strategic Communication," *Military Review* (July/August 2007): 61.
15. Defleur and Ball-Rokeach, 304.
16. Halloran, 13.
17. Ibid., 14.
18. Defleur and Ball-Rokeach, 186.
19. Ibid, 282.
20. Ibid., 285
21. Ibid., 283.
22. Severin and Tandard, 193.
23. Defleur and Ball-Rokeach, 192.
24. Dr. Corely Dennison, Dean, W. Page Pitt School of Journalism and Mass Communications, Marshall University, telephone interview by author, 9 November, 2007.
25. McQuail, 478.
26. Dennison.
27. Defleur and Ball-Rokeach, 31.
28. U.S. Joint Chiefs of Staff, *Joint Functions*, Joint Publication 3.0 (Washington DC: U.S. Joint Chiefs of Staff, 17 September 2006), III-15.
29. Dale Carnegie, *How to Win Friends and Influence People*, (New York NY: Simon and Schuster, Inc., 1981), 18.

Strategic Communication, Psychological Operations and Propaganda: Is a Unified Strategic Message Possible?

1. Thomas X.Hammes, *The Sling and The Stone: On War in the 21st Century*. (St. Paul MN: Zenith Press, 2004), 207-208.
2. Curtis D. Boyd, "Army IO is PSYOP: Influencing More with Less," *Military Review*, (May-June 2007): 69

3. Nancy Snow, "The Smith-Mundt Act of 1948," *Peace Review*, Vol 10, Issue 4, (Dec 1998): 619. To see just how quickly the topic of influence can devolve into accusations of sinister motives, it is instructive to dissect the logic of some activists. Nancy Snow points out that a "particular branch of foreign affairs [called] 'public diplomacy' [Snow's emphasis] is a euphemism for propaganda. The encyclopedia definition of the latter term is 'instruments of psychological warfare aimed at influencing the actions of human beings in ways that are compatible with the national objectives of the purveying state." Note how she first equates public diplomacy with propaganda, a spurious link in itself, but then goes on to define propaganda by its most damning definition, thereby damning by extension any well-intentioned efforts to promote U.S. policy through dialog. It is tempting to dismiss such criticism as the ill-informed commentary of the academic fringe, but such opinions carry significant weight in policy circles. It is in this adversarial environment that the U.S. Government takes hesitant steps toward a sound Strategic Communication policy that achieves national objectives in a way consistent with shared U.S. values.

4. *2006 Quadrennial Defense Review (QDR) Strategic Communication (SC) Execution Roadmap*, Department of Defense, (September 2006), 3.

5. Robert F. Delaney, "Psychological Operations in the 1970s: A Program in Search of a Doctrine," in *DA Pamphlet 525-7-1, The Art and Science of Psychological Operations: Case Studies of Military Application*, Vol I (April 1976), 2.

6. Allen W. Palmer and Edward L. Carter, "The Smith-Mundt Act's Ban on Domestic Propaganda: An Analysis of the Cold War Statute Limiting Access to Public Diplomacy," *Communication Law and Policy* (Winter 2006) available from LexisNexis (accessed June 2007).

7. Ibid, 4.

8. United States Information and Educational Exchange Act, U.S. Code, Sections a and b (1948). The following is an expanded excerpt to show in context the purpose and prohibitions of the law: "(a) Dissemination of information abroad. The Secretary is authorized, when he finds it appropriate, to provide for the preparation, and dissemination abroad, of information about the United States, its people, and its policies, through press, publications, radio, motion pictures, and other information media, and through information centers and instructors abroad. Subject to subsection (b) of this section, any such information (other than "Problems of Communism" and the "English Teaching Forum" which may be sold by the Government Printing Office) shall not be disseminated within the United States, its territories, or possessions, but, on request, shall be available in the English language at the Department of State, at all reasonable times following its release as information abroad, for examination only by representatives of United States press associations, newspapers, magazines, radio systems, and stations, and by research students and scholars, and, on request, shall be made available for examination only to Members of Congress. (b) Dissemination of information within United States. (1) The Director of the United States

Information Agency shall make available to the Archivist of the United States, for domestic distribution, motion pictures, films, videotapes, and other material prepared for dissemination abroad 12 years after the initial dissemination of the material abroad or, in the case of such material not disseminated abroad, 12 years after the preparation of the material."

9. Ibid, 14.

10. U.S. Department of State website, Under Secretary for Public Diplomacy and Public Affairs webpage, http://www.state.gov/r/ (accessed 22 April 2008).

11. Undersecretary of State for Public Diplomacy and Public Affairs Karen Hughes, speech to the Council on Foreign Relations, 10 May 2006, http://www.state.gov/r/us/66098.htm (accessed July 2007).

12. Fred Kaplan, "Karen Hughes, Stay Home! What on Earth is She Doing in the Middle East?" *Slate*, 29 September 2005, http://www.slate.com/id/2127102/ (accessed 23 April 2008). Kaplan makes the following observation regarding Karen Hughes's visits to the Middle East, which he believes have set the U.S. policy objectives back: "Let's say some Muslim leader wanted to improve Americans' image of Islam. It's doubtful that he would send as his emissary a woman in a black chador who had spent no time in the United States, possessed no knowledge of our history or movies or pop music, and spoke no English beyond a heavily accented "Good morning." Yet this would be the clueless counterpart to Karen Hughes, with her lame attempts at bonding….and her tin-eared assurances that President Bush is a man of God."

13. Congress, House, Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee of Appropriations, *US Public Diplomacy: State Department Efforts Lack Certain Communication Elements and Face Persistent Challenges*, Testimony of Jess T. Ford, Director International Affairs and Trade (Washington DC: U.S. Government Accountability Office, 3 May 2006).

14. Advisory Group on Public Diplomacy for the Arab and Muslim World, *Changing Minds Winning Peace: A New Strategic Direction for U.S. Public Diplomacy in the Arab and Muslim World* (Washington DC, 1 October 2003), 16.

15. Ibid, 9.

16. Ibid, 64.

17. Stephen Johnson and Helle Dale, "How to Reinvigorate U.S. Public Diplomacy," *American Diplomacy*, (Heritage Foundation, 2003) www.heritage.org/Research/PublicDiplomacy/bg1645.cfm (accessed 28 April 2008).

18. William P. Kiehl, "Can Humpty Dumpty Be Saved," http:\\www.publicdiplomacy.org/24.htm (accessed 28 April 2008).

19. DoD Directive Number 5148.11, 21 May 2004, 4.

20. "Policy in the Twenty First Century," *Defense Link*, http://www.defenselink.mil/policy/sections/policy_offices/solic/index.html (accessed 23 April 2008).

21. U.S. Strategic Command, http://www.stratcom.mil/about.html (accessed 22 April 2008).

22. *USSOCOM 2007 Posture Statement*, (Fort Bragg, N.C.: U.S. Department of the Army) (internet accessed February 2008), 6.

23. Dennis M. Murphy, "National and Theater Strategic Communication: Organizations, Processes and Emerging Initiatives," presentation to *Strategic Communication* elective at U.S. Army War College, Carlisle Barracks PA, 16 July 2008.

24. 2008 Strategic Communication Guide, (Washington, D.C., U.S. Department of the Army), available from https://akocomm.us.army.mil/2008scg (accessed 21 April 2008).

25. *Quadrennial Defense Review* (Washington DC, U.S. Department of Defense.: February 6, 2006), 92.

26. Gail Hopkins, "Executive Summary of USSOCOM brief to CSA," memorandum, Washington DC, 22 November 2005.

27. Department of the Army, *Information Operations Doctrine: Tactics, Techniques, and Procedures*, Field Manual 3-13 (Fort Leavenworth, KS: U.S. Department of the Army, November 2003), para 2-17.

28. Department of the Army, *Psychological Operations*, Field Manual 3-05.30 (Fort Bragg NC: U.S. Department of the Army, April 2005), para 6-15.

29. Department of the Army, *Operations*, Field Manual 3-0 (Fort Leavenworth KS: U.S. Department of the Army, February 2008), para 7-10.

30. Ibid, para 7-16.

31. Ibid, para 7-30.

Improving the United States' Strategic Communication Strategy

1. Center for Strategic and International Studies, *CSIS Commission on Smart Power: A Smarter, More Secure America* (Washington DC: CSIS Press, 2007), 17.

2. Dennis Murphy and James White, "Propaganda: Can a Word Decide a War?," *Parameters* 37 (Autumn 2007): 23.

3. Joel Roberts, *Winning the Battle of Ideas in the War on Terrorism*, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 14 March 2007), 3.

4. U.S. Department of State, "Country's First National Strategic Communications Plan Presented," *Public Diplomacy Update*, 2, no. 3 (2007): 6.

5. Ibid.

6. National Security Council Strategic Communication and Public Diplomacy Policy Coordination Committee, *U.S. National Strategy for Public Diplomacy and Strategic Communication* (Washington DC: The National Security Council, May 2007), 3.

7. Ibid., 4-5.

8. Ibid., 6-7.

9. Ibid.

10. George W. Bush, *The National Security Strategy of the United States of America* (Washington DC: The White House, September 2002), 31.

11. U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Strategic Communication* (Washington DC: U.S. Department of Defense, September 2004), 24.

12. Ibid., 24.

13. Arnold Abraham, *The Strategic Communication Process: How to Get Our Message Out More Effectively*, National War College Paper (Washington DC: National Defense University, n.d.), 2.

14. George W. Bush, "Establishing the Office of Global Communications," *Executive Order 13283* (Washington DC: The White House, 21 January 2003).

15. Karen Hughes, "Strategic Communication and Public Diplomacy: Interagency Coordination," remarks to the Department of Defense Conference on Strategic Communication, Washington DC, 11 July 2007, linked from the U.S. Department of State web page, http://www.state.gov/r/us/2007/88630.htm (accessed 19 December 2007).

16. Karen Hughes, "Testimony before the House Committee on Appropriations, Subcommittee on State, Foreign Operations, and Related Programs," 19 April 2007, linked from the U.S. Department of State web page, http://www.state.gov/r/us/2007/ 83269.htm (accessed 3 December 2007).

17. Ibid.

18. Ambassador Brian Carlson, Department of State-Department of Defense Liaison, Office of the Under Secretary of State for Public Diplomacy and Public Affairs, telephone interview by author, 8 January 2008.

19. U.S. Department of Defense, *Quadrennial Defense Review Strategic Communication Execution Roadmap*, (Washington DC: U.S. Department of Defense, September 2007), 3.

20. Richard Josten, "Strategic Communication: Key Enabler for Elements of National Power," *IO Sphere* (Summer 2006): 17.

21. Jesse Bourque, "The Language of Engagement: Influence and the Objective," *Journal of Electronic Defense* 30 (November 2007): 34.

22. Dennis Murphy, "The Trouble with Strategic Communication(s)," briefing slides with commentary, Center for Strategic Leadership, Carlisle Barracks PA, 8 November 2007.

23. Richard Halloran, "Strategic Communication," *Parameters* 37 (Autumn 2007): 6.

24. Jeryl Ludowese, *Strategic Communication: Who Should Lead the Long War of Ideas?*, Strategy Research Project (Carlisle Barracks PA: U.S. Army War College, 15 March 2006): 3.

25. Robert Neilson and Daniel Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* 5 (Autumn 1999): 40.

26. Roberts, 7-8.

27. Carnes Lord, *Losing Hearts and Minds? Public Diplomacy and Strategic Influence in the Age of Terror* (Westport CT: Praeger Security International, 2006), 74.

28. Defense Science Board Task Force on Strategic Communication.

29. Carlson.

30. Murphy and White, 17.

31. Ludowese, 4.

32. Bruce Gregory, *Public Diplomacy and Strategic Communication: Cultures, Firewalls, and Imported Norms* (Washington DC: George Washington University, 31 August 2005): 13.

33. Ludowese, 6.

34. Defense Science Board Task Force on Strategic Communication, 7.

35. Curtis Jenkins, "Taking the Communication High Ground: The Case for a Joint Inter-Agency Task Force for Strategic Communication," *DISAM Journal of International Security Assistance Management* 29 (July 2007): 37.

36. Gregory, 33.

37. Foreign Affairs Reform and Restructuring Act, FAIR Act, Public Law 105-277, 105th U.S. Congress, 2nd sess., 1998.

38. Lord, 67.

39. Ibid., 71.

40. Ibid., 74.

41. Murphy and White, 22.

42. Halloran, 8.

43. Jeffrey Feldman, comments during discussions on strategic communication, Carlisle Barracks, U.S. Army War College, 8 January 2008.

44. Linda Robinson, “The Propaganda War,” *U.S. News & World Report*, 29 May 2006, 31.

45. Thomas X. Hammes, a recently retired USMC colonel, has written extensively on 21st century warfare. He categorizes warfare into generations. First Generation Warfare (1GW) was that of the line and column of massed infantry formations when nation-states emerged and up through the Napoleonic Wars. Second Generation Warfare (2GW) was that of massed formations, but with armies entrenched in defensive positions supported by the increased firepower of cannon and automatic weapons as nation-states fully mobilized their populations for total war into the time of WWI. Third Generation Warfare (3GW) was that of movement and firepower with armies moving rapidly through or around their enemies using mechanized formations, improved artillery, and airpower beginning in the final months of WWI and culminating in the Gulf War of 1991. Fourth Generation Warfare (4GW) is that of irregular warfare in which small quasi-military organizations combat traditional nation-state forces using guerrilla tactics, political subversion, terrorism, and most importantly information operations designed to defeat the enemy’s will to continue the fight.

46. Thomas X. Hammes, *The Sling and The Stone: On War in the 21st Century* (St. Paul MN: Zenith Press, 2006), 216.

47. Linton Wells II, *Strategic Communication and the Battle of Ideas: Winning the Hearts and Minds in the Global War on Terrorists*, Statement presented to the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats and Capabilities, 110th Congress, 1st sess., 11 July 2007.

48. Carlson.

49. Ibid.

50. Paul Brown, “New York City Trip Backbrief,” commentary, Carlisle Barracks, U.S. Army War College, 19 November 2007.

51. Carlson.

52. U.S. Government Accountability Office, *Actions Needed to Improve Strategic Use and Coordination of Research* (Washington DC: U.S. Government Accountability Office, July 2007).

53. U.S. Department of State, “Disney Parks and Resorts Partners with Departments of State and Homeland Security to Welcome International Visitors to the United States,” *Public Diplomacy Update*, United States Department of State, 2, no. 4 (2007): 1.

54. Hughes, Testimony, 19 April 2007.

55. Murphy and White, 25.

56. Ibid., 24.

57. David Kilcullen, “Counterinsurgency in Iraq: Theory and Practice, 2007,” briefing slides, September 2007.

58. Steve McClellan, "U.S. Acquires a Taste for Communications Planning," *Adweek*, 6 November 2006, 11.

Bridging the Cultural Communication Gap between America and Its Army

1. U.S. Department of the Army, *The Army*, Army Field Manual 1 (Washington DC: U.S. Department of the Army, 14 June 2001), 32.
2. The Honorable Ike Shelton (D-MO), "Skelton Delivers Address at Historic Westminster College," press release, 3 April 2007, in U.S. Army War College, AY2008 National Security Policy and Strategy Course (Carlisle Barracks: U.S. Army War College, 2007), 31.
3. Charles C. Moskos, John Allen Williams, and David R. Segal, *The Postmodern Military: Armed Forces after the Cold War* (New York: Oxford University Press, 2000), 19-20.
4. Thomas E. Ricks, *Making of the Corps* (New York: Scribner, 1997), 274-275.
5. Michal J. Burbach, *Public Affairs into the 21st Century*, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 29 April 1999).
6. Ricks, 23.
7. Richard Halloran, "Strategic Communication," *Parameters* 37 (Autumn 2007): 6.
8. Mady Wechsler Segal and Chris Bourg, "Professional Leadership and Diversity in the Army," Lloyd J. Mattews, ed., *The Future of the Army Profession*, 2nd ed., rev. and exp. (McGraw-Hill Custom Publishing, 2005), 705.
9. Francis J. Harvey and Peter J. Schoomaker, *Call to Duty, Boots on the Ground A Statement on the Posture of the United States Army*, Fiscal Year 2007, Posture Statement presented to the 110th Cong., 1st sess. (Washington, D.C.: U.S. Department of the Army, 2007), ii.
10. Ibid., C-1.
11. Thomas S. Langston, "The Civilian Side of Military Culture," *Parameters* 30 (Autumn 2000): 25.
12. Linda Lyons, "Teen Views on War, Military Service, Education and Youth," *The Gallup Poll*, 11 March 2003, [article on-line], http://www.gallup.com/poll/7966/Teen-Views-War-Military-Service.aspx (accessed 11 December 2007).
13. Neil Howe and William Strauss, *Millennials Rising: The Next Great Generation* (New York: Vintage Books, 2000), 4.
14. Ellen Neuborne and Kathleen Kerwin, "Today's Teens — The Biggest Bulge Since the Boomers — May Force Marketers to Toss Their Old Tricks," *Business Week*, 15 February 1999 [journal on-line], http://www.businessweek.com/1999/99_07/b3616001.htm (accessed 15 November 2007).

15. Jeffrey M. Jones, "Many Americans Reluctant to Support Their Child Joining Military, Nearly Half Would Suggest a Different Occupation," *The Gallup Poll*, 22 June 2005, [article on-line], http://www.gallup.com/poll/17026/Many-Americans-Reluctant-Support-Their-Child-Joining-Military.aspx (accessed 22 November 2007).

16. Harvey and Schoomaker, C-2.

17. Ibid., 8.

18. Frank Hoffman, "Bridging the Civil-Military Gap," *Armed Forces Journal* (December 2007): 19.

19. Don M. Snider and Gayle L. Watkins, "The Future of Army Professionalism: A Need for Renewal and Redefinition," *Parameters* 30 (Autumn 2000): 8.

20. Segal and Bourg, 706.

21. Ibid., 710.

22. George R. Mastroianni, "Occupations, Cultures, and Leadership in the Army and Air Force," *Parameters*, Winter 2005-06 [journal on-line]; available from http://www.carlisle.army.mil/usawc/Parameters/05winter/mastroia.htm (accessed November 26, 2007).

23. U.S. Army War College Strategic Leadership Course, "Organizational Theory," (Carlisle Barracks: U.S. Army War College, 26 September 2007), 157.

24. John A. Nagle, *Learning to Eat Soup with a Knife, Counterinsurgency Lesson from Malaya and Vietnam* (Chicago: The University of Chicago Press, 2002), 215.

25. U.S. Department of the Army, *Army Leadership*, FM 6-22 (Washington, D.C.: U.S. Department of the Army, 31 August 1999), 2-7.

26. Snider and Watkins, 10.

27. Langston, 26-27.

28. Hoffman, 19.

29. Josh White, "Army off Target on Recruits — Percentage of High School Graduates Drops to New Low," *The Washington Post*, 23 January 2008 [newspaper on-line]; available from http://ebird.afis.mil/ebfiles/e20080123575027.html (accessed 23 January 2008).

30. Segal and Bourg, 706.

31. Ricks, 287.

32. Mastroianni.

33. Ibid.

34. Richard D. Lewis, *When Cultures Collide* (Boston: Nicholas Brealey Publishing, 1996), 179-86.

35. Leonard Wong, “Why Professionals Fight: Combat Motivation in the Iraq War,” Lloyd J. Matthews, ed., *The Future of the Army Profession*, wd ed., rev. and exp. (Boston: McGraw-Hill Custom Publishing, 2005), 505.

36. Lydia Saad, “Military Again Tops ‘Confidence in Institutions’ List, Ratings of the President, Congress, and the Supreme Court are all down,” *The Gallup Poll*, 1 June 2005, [article on-line]; available at http://www.gallup.com/poll/16555/Military-Again-Tops-Confidence-Institutions-List.aspx (accessed 1 December 2007).

37. Snider and Watkins, 10.

38. Hoffman, 19-20.

39. Peter A. Gudmundsson, “America’s Upper Classes Have Gone AWOL,” *Christian Science Monitor*, 8 January2008, [newspaper on-line]; available from http://ebird.afis.mil/ ebfiles/e20080108571889.html (accessed 8 January 2008).

40. Secretary of Defense Robert M. Gates, *Remarks as Delivered at Kansas State University*, Manhattan, KS, Monday, 26 November 2007, http://www.defenselink.mil/speeches/speech.aspx?speechid=1199 (accessed 1 December 2007).

41. Halloran, 9.

42. Center for Disease Control, “Six Critical Health Behaviors,” 13 November 2007 [study on-line], http://www.cdc.gov/HealthyYouth/healthtopics/ (accessed 13 November 2007).

43. Dennis M. Murphy and James F. White, “Propaganda: Can a Word Decide a War?” *Parameters* 37 (Autumn 2007): 25.

44. Segal and Bourg, 705.

45. Ibid., 706.

46. Ibid., 707.

47. Charles C. Moskos and John Sibley Butler, *All That We Can Be, Black Leadership and Racial Integration the Army Way* (New York: Basic Books, 1996), xiii.

48. BG David A. Fastabend and Mr. Robert H. Simpson, “Adapt or Die, The Imperative for a Culture of Innovation in the United States Army” in the U.S. Army War College AY 2008 Strategic Thinking Course (Carlisle Barracks: U.S. Army War College AY 2008 Strategic Thinking Course), 148.

49. Peter M. Senge, *The Fifth Discipline: The Art and Practice of The Learning Organization* (New York: Doubleday, 1990), 3.

50. Sun Tzu, *The Art of War* (London: Oxford University Press, 1963), 84.

Section Two – Information Effects in the Physical Domain

Introduction

1. Deputy Secretary of Defense, Gordon England, "The Definition of 'Cyberspace,'" memorandum for Secretaries of the Military Departments, et al, (Washington, DC: May 12, 2008).
2. Vice Chairman of the Joint Chiefs of Staff, General James E. Cartwright, "Definition of Cyberspace Operations," action memo for Deputy Secretary of Defense, (Washington, DC: September 29, 2008).
3. Robert M. Gates, *National Defense Strategy* (Washington, DC: Department of Defense, June 2008), 18.
4. Clay Wilson, CRS Report to Congress. Network Centric Warfare: Background and Oversight Issues for Congress.Congressional Research Service, CRS-RL32411 (Washington, DC: Library of Congress, March 18, 2005), CRS-2.
5. Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, "CJCS Guidance for 2008-2009," memorandum for the Joint Staff, (Washington, DC: November 18, 2008), 4.

Unmanned Aircraft Systems Role in Network Centric Warfare

1. George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: The White House, 16 March 2006), 43.
2. U.S. Department of Defense, Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, D.C.: U.S. Department of Defense, 5 January 2005), 6.
3. Ibid., 7.
4. John Keller, "Defense spending set to increase for electronics and electro-optics programs in 2007," *Military and Aerospace Electronics*, March 2006, http://mae.pennnet.com/articles/article_display.cfm?ARTICLE_ID=250344&p=32&section=ARTCL&subsection=none&c=none&page=1 (accessed 13 January 2008).
5. U.S. Department of Defense, *The Quadrennial Defense Review Report* (Washington, D.C.: U.S. Department of Defense, 6 February 2006), 58. (hereafter cited as 2006 QDR)
6. John McHale, "Market Analysts See Strong Growth for UAV Market," *Supplement to Military and Aerospace Electronic*s, August 2006, http://mae.pennnet.com/articles/article_display.cfm?Section=ARTCL&C=UnVSt&ARTICLE_ID=263107&KEYWORDS=uav%20market&p=32 (accessed 20 January 2008).

7. U.S. Department of Defense, Unmanned Systems Roadmap, 2007-2032 (Washington, D.C.: U.S. Department of Defense, 2007), 19. (hereafter cited as Unmanned Systems Roadmap)

8. Ibid., 20.

9. U.S. Government Accountability Office, *Unmanned Aircraft Systems: Advanced Coordination and Increased Visibility Needed to Optimize Capabilities: Testimony to the Subcommittee on Air and Land Forces*, Committee on Armed Services, House of Representatives (Washington, D.C.: U.S. Government Accountability Office, July 2007), 2.

10. Ibid., 2.

11. This paper does not seek to examine in detail the technical composition, variants, and operational capabilities of all UAS. Rather, it provides fundamental understanding of UAS to ensure necessary background. See Unmanned Systems Roadmap, Appendix A, for a listing of numerous programmed and experimental UAS to include their background, characteristics, and performance data.

12. Air, Land, and Sea Application Center, *UAS: Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems* (Langley Air Force Base: Air, Land, and Sea Application Center, 3 August 2006), I-2 to I-3.

13. Ibid., I-5 to I-6.

14. 2006 QDR, vii-viii.

15. U.S. Government Accountability Office, *Unmanned Aircraft Systems: Advanced Coordination*, 10-11.

16. U.S. Joint Chiefs of Staff, Joint Publication 3-0, Joint Operations, defines the Global Information Grid (GIG) as "the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, and security services, other associated services, and National Security Systems."

17. Captain Elizabeth Culbertson, "Unmanned Aircraft Key to Future Operations, General Says," *Armed Forces Press Service*, 20 October 2006, http://www.defenselink.mil/news/newsarticle.aspx?id=1730 (accessed 5 November 2007).

18. U.S. Government Accountability Office, *Unmanned Aircraft Systems: Advanced Coordination*, 6.

19. Air, Land, and Sea Application Center, III-6.

20. U.S. Government Accountability Office, *Unmanned Aircraft Systems: DOD Needs to More Effectively Promote Interoperability and Improve Performance Assessments: Report to the Subcommittee on Tactical Air and Land Forces, Committee on*

Armed Services, House of Representatives (Washington, D.C.: U.S. Government Accountability Office, December 2005), 2.

21. Kevin J. Cogan and Dr, Jeffrey L. Groh, "Network-Centric Operations: Getting 'IT' Right," *NECWORKS*, no.2 (2007), 30.

22. U.S. Government Accountability Office, *Unmanned Aerial Vehicles: Major Management Issues Facing DOD's Development and Fielding Efforts, Testimony to the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives* (Washington, D.C.: U.S. Government Accountability Office, March 2004), 3.

23. Dyke D. Weatherington, "Unmanned Aircraft Systems Task Force," briefing slides, Pentagon, OUSD(AT&L)/PSA/Air Warfare, 6 November 2007.

24. Unmanned Systems Roadmap, 1.

25. Stephen Mundt, Brigadier General, *Statement of Stephen Mundt, Director, Army Avaition Directorate, United States Army before the Committee on House Armed Services Subcommittee on Tactical Air and Land Forces, U.S. Congress, House, Committee on House Armed Services Subcommittee of Tactical Air and Land Forces*, April 6 2006.

26. Ibid.

27. Unmanned Systems Roadmap, 4.

28. Kris Osborn, "U.S. Aviators, UAVs Team Up Against IEDs," *Defense News*, January 21, 2008, http://ebird.afis.mil/cgi-bin/ebird/displaydata.pl?Requested=/ebfiles/ e20080120574598.html (accessed 21 January 2008).

29. Ibid, 65.

30. U.S. Air Force Fact Sheet, "Global Broadcast Service (GBS) Joint Program," February 2007, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=7853 (accessed 7 November 2007).

31. Jeffrey L. Groh, "Network-Centric Warfare: Just About Technology?," in *The U.S. Army War College Guide to National Security Policy and Strategy*, ed. J. Boone Bartholomees, Jr. (Carlisle Barracks: U.S. Army War College, June 2007), 380.

32. U.S. Department of the Army, 2007 Army Modernization Plan (Washington D.C.: U.S. Department of the Army, 5 March 2007), 152. See also U.S. Army Signal Center, *Capability Development Document for Warfighter Information Network-Tactical (WIN-T)* (Fort Gordon: U.S. Army Signal Center, 6 November 2006), i and 35.

33. Top three Mission Areas are Reconnaissance, Precision Target Location and Designation; and Signals Intelligence, *Unmanned Systems Roadmap*, 21.

34. U.S. Army Training and Doctrine Command, *Force Operating Capabilities*, TRADOC Pamphlet 525-66 (Fort Monroe: U.S. Army Training and Doctrine Command, 1 July 2005), 21.

35. Donald H. Rumsfeld, *The National Defense Strategy of the United States of America* (Washington D.C.: The Pentagon, March 2005), 14.

36. U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations Version 2.0* (Washington D.C.: U.S. Joint Chiefs of Staff, August 2005) 21.

37. Kris Osborn, "U.S. Army Faces Spectrum Crunch," *Defense News*, January 7, 2008, http://ebird.afis.mil/ebfiles/e20080106571436.html (accessed 7 January 2008).

38. General Dynamics C4 Systems, *Warfighter Information Network-Tactical: No-Air-Tier STUDY Final Repor*t, prepared for Department of the Army Project Manager Warfighter Information Network-Tactical, (Taunton, MA: General Dynamics C4 Systems, 13 September 2005), 69.

39. U.S. Army Signal Center and Fort Gordon, *Initial Capabilities Document for Aerial Layer Network Transport* (Fort Gordon: U.S. Army Signal Center and Fort Gordon, 3 August 2007), 5.

40. Stephen Trimble, "Seamless Airborne Networks Are Becoming a Reality Thanks to Bridging Technology," *Jane's Defense Weekly*, 24 January 2007, http://integrator.hanscom.af.mil/2007/January/01252007/012522007-15.htm (accessed 19 December 2007).

41. Otto Kreisher, "In Demand," *Navy League of the United States*, November 2005, http://www.navyleague.org/Sea_power/nov05-10.php (accessed 24 October 2007).

42. Program Manager for UAS recently delivered two Communication Relay Package-Light payloads for the 25th Infantry Division's Shadow UAS. These systems are successfully operating in Iraq and provide FM communications extension up to 170 kilometers. See Jeremy Vigna and Gene Cantrell, "Shadow-Tactical Unmanned Aircraft System Communication Relay Package-Light," *Army Communicator* 32, no. 4 (Fall 2007): 18.

43. Mundt.

44. U.S. Department of the Army, *2007 Army Modernization Plan* (Washington D.C.: U.S. Department of the Army, 5 March 2007), 7-8. See also http://www.army.mil/fcs/ which provides information on the Army's Future Combat System program.

45. The United States Army Future Combat System Homepage, http://www.army.mil/fcs/network.html (accessed 20 December 2007).

46. U.S. Government Accountability Office, *Unmanned Aircraft Systems: Advanced Coordination*, 10.

47. Donna Miles, "Spectrum Summit Focuses on Current, Future Warfighter Needs," *Defense Link News Article*, 7 December 2006, http://www.defenselink.mil/news/ newsarticle.aspx?id=2345 (accessed 17 January 2008).

48. Maryann Lawlor, Spectrum Management Advances in the Queue," *Signal* 62, (December 2007): 46-47.

49. Rick Atkinson, "'If You Don't Go After the Network, You're Never Going to Stop These Guys. Never." *The Washington Post*, 3 October 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366.html?sid=ST2007092900754 (accessed 3 October 2007).

50. David Milburn, "Unmanned Aircraft Systems," briefing slides, Redstone Arsenal, UAS Project Manager, 1 February 2007.

51. *Unmanned Systems Roadmap*, 47.

52. Defense Spectrum Office, "Findings and Recommendations of the Study On: 'Early Consideration of Spectrum Supportability in Spectrum Dependant System Acquisitions'," 27 September 2005, https://acc.dau.mil/GetAttachment.aspx?id=21871&pname=file&lang=en-US&aid=2053 (accessed 1 November 2007), 4.

53. Lawlor, 44.

54. U.S. Government Accountability Office, *Unmanned Aircraft Systems: Advanced Coordination*, 11.

55. Paige Atkins, "Spectrum Guide: Developing Innovative Solutions to Ensure Global Access," interview by Harrison Donnelly, Military Information Technology 11, no.10 (2007), 25.

56. U.S. Army Signal Center and Fort Gordon, 4.

57. DoD is currently developing spectrum management tools that bear potential in fulfilling this recommendation. The Coalition Joint Spectrum Management Planning Tool (CJSMPT) is currently undergoing field testing. If successful, CJSMPT would serve as the first increment to a formal DoD program called the Global Electromagnetic Spectrum Information System (GEMSIS). See Michael Burnett, Tool for a Crowded Spectrum, *Military Information Technology* 11, no. 10 (2007), 9.

Blue Force Tracking: Building a Joint Capability

1. Daniel Gonzales, John Hollywood, and Sarah Harting, *Legacy Assessment of Ground Blue Force Tracking Systems* (Arlington, VA: RAND National Defense Research Institute, 2007), 25.

2. Bryon Greenwald, "Joint Capability Development," *Joint Forces Quarterly*, no. 44 (1st quarter 2007): 51.

3. Chairman of the Joint Chiefs of Staff, Instruction 8910.01A, *Joint Blue Force Situational Awareness Operations Guidance*, April 30, 2004, current as of March 20, 2007, x.

4. Lieutenant Colonel Sandy Yanna, *Comments on OUSD(AT&L)'s Legacy Assessment of Ground Blue Force Tracking Systems* (U.S. Army Space and Missile Defense Command, Joint Blue Force Situational Awareness Mission Management Office, 2007): 2.

5. CJCSI 8910.01A, 3.

6. Combat Identification (CID) is the process of attaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high-confidence, real-time application of tactical options and weapon resources can occur. The objective of CID is to maximize combat/mission effectiveness while reducing total casualties (due to enemy action and fratricide).

7. Lieutenant Michael Sweeney, "Blue Force Situational Awareness Capability" briefing slides, HQ, U.S. Marine Corps, Arlington, Va, 30 June 2004.

8. Gonzales, Hollywood and Harting, 17.

9. Ibid., 15

10. Yanna, 3.

11. Lieutenant General James Cartwright, USMC, JROCM 161-03, Blue Force Tracking Memorandum for: Vice Chief of Staff, US Army and Assistant Commandant of the Marine Corps, The Joint Staff, Washington, D.C. 13 August 2003

12. Lieutenant Colonel Jim Smith, USA, Lieutenant Colonel Mike Sweeney, USMC, "Adopting Joint, Interoperability Through Convergence," Defense Acquisition University, AT&L (September-October 2005): 33-37.

13. Joint Capability Technology Demonstrations, http://www.acq.osd.mil/jctd (accessed 8 January, 2008).

14. The Urgent Needs Statement process was designed to provide rapid acquisition of a capability in order to meet an urgent requirement. Resourcing of a solution is not limited to existing program of records. The acceleration of an Advanced Concept Technology Demonstration (ACTD) is often used to meet the requirement. The increased use of this process has complicated efforts to enhance interoperability.

15. Gonzales, Hollywood and Harting, 105.

16. Peter Anderson, Compute Systems Center Incorporated, "Systems Interoperability, MAGTF C2 Options," Quantico, Virginia, Marine Corps Combat Development Command, 16 October 2007.

17. Lieutenant General Larry J. Dodgen, "U.S. Army, Space: Inextricably Linked to Warfighting," Military Review (January-February 2006): 88.

18. Gonzales, Hollywood and Harting, 25.

19. William J. Bayles, "The Ethics of Computer Network Attack," *Parameters* (Spring 2001): 44-46.

20. David W. Tarr, *Military Technology and the Policy Process*, University of Wisconsin, 139.

21. Joint Forces Command, "Blue Force Tracking (BFT) Position Location Information (PLI) Security and Classification Policy Briefing to the JROC," briefing slides without scripted commentary (Pentagon, Arlington VA, 31 January 2008).

22. Defense Information Systems Agency, http://www.disa.mil/gccs-j/index.html (accessed 20 November 2007).

23. JROCM 161-03 directed that the U.S. Army and U.S. Marine Corps develop a plan to converge existing programs of record into a single capability. Although some progress has been made in sharing data, true convergence has not been accomplished to date.

24. United States Joint Forces Command home page, http://www.jfcom.mil/about/priorities.htm (accessed 12 January, 2008).

25. Lorenzo Cortes, "Pace Asserts JROC's Importance in Developing CONOPS," *Defense Daily*, (Jan 24, 2003), 1.

26. Ibid., 1.

27. United States Joint Forces Command, *Command Mission and Strategic Goals*, http://www.jfcom.mil/about/priorities.htm.

28. Joint Forces Command, "Blue Force Tracking (BFT) Position Location Information (PLI) Security and Classification Policy Briefing to the JROC," briefing slides without scripted commentary (Pentagon, Arlington VA, 31 January 2008).

29. Jen DiMascio, "Skelton to Press Pentagon to Start Roles and Missions Review," *Defense Daily*, 24 January 2008, x.

30. Gonzales, Hollywood and Harting, 15.

31. DARPA web site, http://www.darpa.mil/darpatech99/presentations/scripts/ato/reichlen.we.txt.

32. Richard J. Dunn, III "Blue Force Tracking, The Afghanistan and Iraq Experience and Its Implications for the U.S. Army," *Northrop Grumman Mission Systems* (2005): 13.

Providing an Enterprise Service Architecture to the Net-Centric Warfighter

1. MG Carroll F. Pollett, Commander NETCOM, "Strengthening Operational Responsiveness and Security," *Military Information Technology Online*, LandWarNet Transformer, http://www.military-information-technology.com/article.cfm?DocID=2142 (accessed 23 November 2007).

2. VADM Nancy Brown, Director, C4 Systems, Joint Staff J6, Command Control, Communications and Computer Systems Directorate, "Joint Net-Centric Operations Campaign Plan," http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf (accessed 5 January 2008).

3. Ibid.

4. U.S. Joint Forces Command, "Standard Operating Procedure & Tactics, Techniques, and Procedures for the Standing Joint Force Headquarters Core Element" (14 December 2004), 4.

5. U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45, (HQ Department of the Army, Washington DC) http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf (accessed 23 November 2007).

6. Brown.

7. Ibid.

8. U.S. Army Chief Information Office, The Army Knowledge Management, Strategic Plan, 2nd ed. (Washington, D.C.: U.S. Government Printing Office, 2003), 1-4.

9. U.S. Department of the Army, *Joint Operations,* Joint Publication 3.0 (Washington, D.C.: U.S. Department of the Army), available from http://www.dtic.mil/doctrine/jel/new_pubs/ jp3_0.pdf; Internet; accessed 2 February 2008.

10. U.S. Department of the Army, Signal Support to Theater Operations, Field Manual Interim 6-02-45 (Washington, D.C.: U.S. Department of the Army), http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf (accessed 20 November 2007).

11. Joint Operations Concepts, "An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution In the 21st Century," https://augateway.maxwell.af.mil/affor/text/evolve/joc.htm (accessed 15 January 2008).

12. Microsoft overlays the generic domain structure with architecture described as "Forests and trees," where the trees are individual domains and a Forest consists of a group of domains, who selectively share a common set of trusts and applications. Each Forest has an Active Directory service that lists all of the users and applications as well as who, according to the Access Control List, is allowed to connect to whom within the Forest.

13. U.S. Department of Defense, *Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise*, Version 1.0, http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf (accessed 17 January 2008).

14. U.S. Department of Defense, *Active Directory Security Technical Implementation Guide*, Version 1, Rel. 1, http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf (accessed 19 January 2008).

15. Ibid.

16. LandWarNet is the Army's portion of the Global Information Grid (GIG) supporting users around the world. LandWarNet is the combination of infostructure and services across the Army. It provides for processing, storing, and transporting information over a seamless network. It is the Army counterpart to the Air Force ConstellationNet and the enterprise network of the Navy's ForceNet.

17. For background on the GIG see U.S. Department of Defense, Defense Information Systems Agency, *GIG Bandwidth Expansion*, http://www.disa.mil/main/prodsol/gig_be.html (accessed 3 January 2008).

18. U.S. Department of the Army, United States Army Signal Center, Directorate Of Combat Developments Concepts and Doctrine Division, *Concept for Implementation of Active Directory in Tactical Army Units*, Version 1.0 (Washington DC: U.S. Department of the Army, 10 July 2006), iii.

19. The "NIPRNET," the unclassified but sensitive Internet protocol router network (formerly called the Non-secure Internet Protocol Router Net), is a network of Internet protocol routers owned by the Department of Defense. Created by the Defense Information Systems Agency (DISA), NIPRNET is used to exchange unclassified but sensitive information between "internal" users. It can thus be distinguished from the Secret Internet Protocol Router Network (SIPRNET), which is used by the DoD to exchange classified information in a totally secure environment.

20. Ibid.

21. Ibid., 1.

22. For background on the Microsoft Forest and Active Directory Design, see Microsoft Technet, Microsoft Windows Server 2003 Active Directory, http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx (accessed 3 January 2008).

23. U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45 (U.S. Department of the Army, Washington DC) http://www.fas.org/ irp/DODdir/army/fmi6-02-45.pdf (accessed 20 November 2007).

24. Vice Admiral Brown, the previous C6 for the Multi-National Forces–Iraq (MNF-I), now serves as the Director for Command, Control, Communications and Computer (C4) Systems (J-6), the Joint Staff, Washington DC.

25. Maryann Lawlor, "Transforming through Jointness," *Signal*, 61, 66-68, 70 (June 2007) [journal online] available from ProQuest (accessed 6 February 2008).

26. U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, *Concept for Implementation of Active Directory in Tactical Army Units*, Version 1.0 (Fort Gordon, 10 July 2006), iii.

27. U.S. Department of the Army, *Concept for Implementation of Active Directory in Tactical Army Units,* (U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon GA), iii.

28. GEN Peter Pace, Chairman of the Joint Chiefs of Staff, *Shaping the Future*, http://integrator.hanscom.af.mil/2005/October/10132005/PaceGuidance02Oct05.pdf (accessed 6 January 2008).

29. Concept for Implementation of Active Directory in Tactical Army Units, A-1.

30. Ibid.

31. Ibid., 12.

32. U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.02, http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf (accessed 27 December 2007).

33. NETCOM/9TH Signal Command (Army) Technical Authority (TA), *Implementation Memorandum U.S. Army Enterprise Systems Technology Activity (ESTA)*, Number 2006-006 (United States Army, Fort Huachuca AZ, June 2006), 9.

34. Ibid.

35. Concept for Implementation of Active Directory in Tactical Army Units, 1-6.

36. Combined Enterprise Regional Information Exchange System (CENTRIXS) is the premier network for coalition interoperability in support of military operations. Ongoing coalition operations continue to test and prove the viability of the CENTRIXS enterprise. Information flow to coalition partners via the multiple versions of CENTRIXS networks achieved unprecedented volume and continues to expand.

37. U.S. Congressional Research Service Report, *Network Centric Warfare: Background and Oversight Issues for Congress*, 2 June 2004, http://www.fas.org/man/crs/RL32411.pdf (accessed 2 February 2008).

38. BG Jeffery Smith stated in his Army Presentation at a recent Microsoft Conference that NSC is a 5 year pay off, and LTG Sorenson briefed it as part of the 10-15 POM for DA G6 in his keynote address.

39. Concept for Implementation of Active Directory in Tactical Army Units, 1-6.

40. Ibid.

41. Ibid., 17.

42. Brent Gatewood, Senior Systems Engineer, Corps Automation Office, HQ V Corps, Heidelberg, Germany; 15 March 2008.

43. U.S. Department of the Army, *Transforming the U.S. Military*, http://www.defenselink.mil/specials/transform/intro.html (accessed 14 October 2008).

44. Lawlor.

45. LTG John R. Vines, U.S. Army, *The XVIII Airborne Corps on the Ground in Iraq*, http://usacac.army.mil/CAC/milreview/English/SepOct06/Vines.pdf (accessed 27 December 2007).

46. U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45 (U.S. Department of the Army, Washington DC), http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf (accessed 20 November 2007).

47. Ibid., 1-2.

48. Ibid.

49. NETCOM/9TH Signal Command (Army) Technical Authority (TA).

50. Sites that provide access to DISN via Defense Satellite Communications (DSCS) X-band terminals.

51. NETCOM, *Army NETOPS CONOPS*, ver 1.0, https://ascp.monmoutharmy.mil/scp/downloads/standardspolicy_files/NETCOM_NETOPS_CONOPS_v10_1.pdf. 2-12.

52. COL Chris Wilhelm, CCJ6 Information Brief to JTF Interoperability Panel (U), Chief, Communications Plans and Operations Division, USCENTCOM CCJ6-C, 9 May 2006.

53. Concept for Implementation of Active Directory in Tactical Army Units, 1.

54. For background on the Microsoft Directory Structures see Microsoft TechNet, *Windows 2003 Resource Kit*, http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/gloss/reskitgloss.mspx?mfr=true (accessed 3 January 2008).

55. Ibid.

56. John Fontana, "Active Directory 'Forests' May Cause Pain," *Network World*, 17 (February 2000): [journal online]; available from ProQuest (accessed 6 February 2008), 16, 124.

57. U.S. Department of Defense, *Active Directory Security Technical Implementation Guide*, Ver. 1, Rel. 1, http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf (accessed 17 January 2008).

58. NETCOM/9TH Signal Command

59. Concept for Implementation of Active Directory in Tactical Army Units, A-1-A-5.

60. Ibid.

61. For background on the Microsoft Directory Structures, see Microsoft TechNet, *Windows 2003 Resource Kit*, http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/gloss/reskitgloss.mspx?mfr=true (accessed 3 January 2008).

62. U.S. Department of Defense, *Active Directory Security Technical Implementation Guide*, Ver. 1, Rel. 1, http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf (accessed 17 January 2008).

63. Ibid.

64. The discussion on the Resource Forest and concept of implementation in Iraq is credited to Automation Services Division for MNC-I during rotation 05-07 supported by the V Corps and the follow-on rotation 05-08 supported by the III Corps. This concept is not officially documented but was approved by the MNC-I Information Services Division Chief during OIF 05-07 and further executed and documented by the MNC-I III Corps.

65. CW2(P) Anthony Dennis, USA, Multi-National Corps Iraq, Information Services Division C6 Services Technician; 14 December 2008.

66. Ibid.

67. Ibid.

68. CW2(P) Anthony Dennis and Mr. Brent Gatewood, USA, Multi-National Corps Iraq, *The Resource Forest Cookbook*, interview by the author, 8 November 2008.

69. Ibid.

70. NETCOM, Army NETOPS CONOPS.

71. Ibid.

72. U.S. Department of Defense, Office of the Chief Information Officer, *Department of Defense Information Sharing Strategy*, http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf (accessed 15 January 2008).

73. Ibid.

74. CW3 Ross Ball, USA, Network Engineer Network Enterprise Technology Command/9th Signal Command Army, interview by the author, 8 February 2008.

Achieving the Department of Defense's Net Centric Vision of Information Sharing while Overcoming Cultural Biases to Control Information

1. Government Accountability Office, "Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information." GAO-06-385, (Washington, D.C: March 2006), 2-3.

2. Strategic Studies Institute, *U.S. Army War College Key Strategic Issues List*, (Carlisle Barracks, PA: July 2007), 53.

3. Assistant Secretary of Defense for Networks and Information Integration, DOD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense" (Washington, D.C: 2 December 2004), 2.

4. Harry R. Yarger, “Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model” (Carlisle Barracks PA: June 2006), 111.

5. Tim Berners-Lee and Mark Fischetti, *Weaving the Web* (New York, NY: HarperCollins Books, 2000), 124.

6. The White House, *The National Security Strategy of the United States of America* (Washington DC: October 2006), 24.

7. The White House, *The National Strategy for Maritime Security* (Washington DC: September 2005), 13-16.

8. Ibid, 16.

9. Chairman of the Joint Chiefs of Staff, *National Strategy to Combat Weapons of Mass Destruction* (Washington, DC: 13 February 2006), 5-26.

10. DoD Directive 8320.2, 2.

11. Assistant Secretary of Defense for Networks and Information Integration, DOD Directive 8320.02-G, “Guidance for Implementing Net-Centric Data Sharing” (Washington DC: 12 April 2006), 9.

12. Assistant Secretary of Defense C3I, DOD Directive 8500.1, “Information Assurance” (Washington, D.C: 24 October 2002), 4.

13. Assistant Secretary of Defense for Networks and Information Integration, DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)” (Washington DC, 5 May 2004), 3.

14. 14DoD Directive 8320.02-G, 11.

15. Ibid, 32.

16. Ibid, 26.

17. The Privacy Act of 1974, 5 U.S.C. § 552a, As Amended, (Washington DC), 464.

18. National Institute of Standards and Technology, FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg MD: February 2004), 1.

19. DoD Directive 8320.2, 2.

20. Rob Fay, “Effective Culture Change in the FBI” (15 June 2005), 2-3.

21. Department of Homeland Security, Securing Our Homeland U.S Department of Homeland Security Strategic Plan (Washington, D.C.: February 2004), 6.

22. Melvin E. Conway, “How Do Committees Invent” *Datamation* (April 1968), 8.

23. Fay, 5-6.

24. Carlos E. Cortés, "Leadership Qualities in a Changing America," Federal Executive Institute Presentation (Charlottesville, VA: March 2006), 1.

25. Christopher Thomas and Milton Ospina, *Measuring Up The Business Case for GIS* (Redlands, CA: ESRI Press. 2004), 18-20.

26. Weaving the Web, 207.

27. Ibid, 237.

28. Tim Berners-Lee, "Semantic Web on XML," XML 2000 (Washington DC: 6 December 2000), 17.

29. Weaving the Web, 189-190.

30. Ibid, 188.

31. Director of National Intelligence, *Intelligence Community Enterprise Architecture: IC EA Conceptual Data Model*, Version 1.2 (Washington DC: 22 August 2006), 32.

32. Paul Shaw, "Semantics of Security," Systems and Software Technology Conference Presentation (Salt Lake City UT: April 2006), 7.

33. Department of Homeland Security, "Fact Sheet: Homeland Security Operations Center (HSOC)" (Washington DC: 8 July 2004), 1.

34. Paul Shaw and David Roberts, "White Paper on the Cross-domain Information Exchange Framework (CIEF): Implementing the Universal Core" (San Diego CA: 14 September 2007), 7.

35. Conway, 7.

36. Edgar M. Johnson, Workshop Introducing Innovation and Risk: Implications of Transformation the Culture of DOD, (Alexandria, VA: Institute for Defense Analyses, 2004), II-2.

37. Christopher H. Baum, *Government Agencies are Data Stewards, Not Owners* (Stamford CT: Gartner Research: 31 December 2004), 4-5.

38. Weaving the Web, 124.

Prudens Futuri